Next Page

OMB Control Number: 0694-0119

Expiration Date: September 30, 2020

DEFENSE INDUSTRIAL BASE ASSESSMENT: USE OF SELECT SOFTWARE IN U.S. INFORMATION COMMUNICATION 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, requested by the Department of Defense and Department of Homeland Security, covers a range of topics including technology sharing, information network devices incorporating software, software design and manufacturing, product end users, and related supply chain issues. Information on company finances, research and development spending, and capital expenditures also is collected in 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 technology is employed in products sold by companies operating in the United States. This data collection will also enable industry and government policy officials to benchmark industry practices and to raise awareness of potential 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 Information furnished herewith is deemed confidential and will not be published or disclosed except in accordance with Section 705 of the Defense Production Act of 1950, as amended (50 U.S.C App.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, DC 20230, and to the Office of Management and Budget, Paperwork Reduction Project (OMB Control No. 0694-0119), Washington, DC 20503.

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

Previous P	age	Next Page
	Table of Contents	
I	Cover Page	
Ш	Table of Contents	
III	General Instructions	
IV	<u>Glossary</u>	
1	Types of Information Network Products Designed, Manufactured and Outsourced	
2	Sources of Software Content & Licensing and Sharing Practices for Information Network Products Designed and Manufactured	
3	Types of U.S. Network Information Network Products Containing XYZ Hardware and Software & Product and Services Collaboration and Development Activities With XYZ Companies	
4	XYZ Technologies Deployed in Company Products & Terms of Technology License	
5	End Users of Hardware and Software Products Sold Containing XYZ Technologies and Operating Sytems	
6	Modes of Accessing XYZ Technologies for Product Development-Production & XYZ Technologies Deployed in Company Products - Clones & Counterfeits	
7	Reasons for Using XYZ Technologies in Company Products	
8	Integration/Embedding of XYZ Technologies - Technology Types/Version Numbers	
9	Integration/Embedding of XYZ Technologies - Functions-Capabilities/Methods	
10	Integration/Embedding of XYZ Technologies - Certs/Interfaces	
11	Integration/Embedding of XYZ Technologies - System Access/Data Access	
12	Integration/Embedding of XYZ Technologies - Functional Conditions for XYZ Technologies/Limits on XYZ in Systems	
13	Product Design, Manufacturing, and Servicing of Products Containing XYZ Technologies - Internal-External/Third Party Services	
14	Integration/Embedding of XYZ Technologies - Telemetry I: Direct Communications, Types of Communications	
15	Integration/Embedding of XYZ Technologies - Telemetry 2: Receiving Methods, Returning Info	
16	Integration/Embedding of XYZ Technologies - Telemetry 3: Passive Indicators, All Indicators	
17	Practices for Tracking Technologies Used In Hardware & Software Network Products Sold By Your Organization	
18	Financials: Sales and Income Statement	
20	Financials: Research & Development and Capital Expenditures	
22	<u>Employment</u>	
23	Competitiveness	
24	Cybersecurity	
25	Certification Page BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act	

Proviou	us Page Next Page
	eral Instructions
Gene	
	Your organization is required to complete this survey on information communication technology hardware and software-related products that your organization has developed, manufactured, or marketed since 2014 using a Microsoft Excel template, which can be downloaded from the BIS website: http://bis.doc.gov/softwaresurvey
А.	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.
	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.
	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.
В.	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.
C.	Do not disclose any classified information in this survey form.
	Questions related to the survey should be directed to BIS survey support staff at softwaresurvey@bis.doc.gov
D.	E-mail is the preferred method of contact.
	You may also speak with a member of the BIS survey support staff by calling (202) 482-7808.
	After completeing, reviewing, and certifying the Excel survey, submit the survey via our Census Bureau web portal:
E.	https://respond.census.gov/softwaresurvey
	Do not submit the survey via email.
	For questions related to the overall scope of this Industrial Base assessment, contact <u>softwaresurvey@bis.doc.gov</u> or:
F.	Brad Botwin, Director, Industrial Studies Office of Technology Evaluation, Room 1093 U.S. Department of Commerce 1401 Constitution Avenue, NW Washington, DC 20230
	DO NOT submit completed surveys to Mr. Botwin's postal or personal e-mail address. All surveys must be submitted via the Census Bureau web portal.
	BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Previous Page Next Page Section: Glossary Glossary Antivirus software detects and removes viruses from computers. It also protects against a range of malicious software, including; keyloggers, Antivirus Scanning Application - Host-based browser hijackers. Trojan horses, worms, rootkits, spyware, adware, botnets and and ransomware. A collection of software that manages computer hardware resources and provides common services for computer programs. **Computer Operating Systems** Source(s): NIST SP 800-152 A systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, Data Loss Prevention (DLP) medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of NSS information. Source(s): CNSSI 4009-2015 A systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest Data Recovery (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Endpoint detection and response tools monitor and record endpoint and network events in a central database to support analysis, detection, investigation, reporting, and alerts. A software agent installed on the host system provides the foundation for event monitoring and reporting. End Point Detection & Response (EDR) Ongoing monitoring and detection is accomplished with analytic tools to support an organization network security by identifying, responding to, and deflecting internal threats and external attacks. A host firewall is a software application or suite of applications installed on a singular computer. Typically, operating system manufacturers include firewall software as part of the system. This is true of Windows (post-Windows 2000), Mac OS X and many distributions of Linux Firewalls - Host/Application Side (Ubuntu, Fedora and SuSE). A personal host firewall is managed on the individual computer where the firewall is installed on. The administrator has to have access to the computer to install and configure the firewall. An inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" Firewalls - Network Side the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall). Source(s): NIST SP 800-82 Rev. 2 A software product that 1) protects the organization's network and users; or 2) protects cloud infrastructure and servers. A cloud firewall operates like an on-premises firewall appliance, except that it is based in the cloud. Service providers call this a software-as-a-service (SaaS) firewall, security as a service (SECaaS), or even firewall as a service (FWaaS). There are also cloud-based services that run in a virtual data Firewalls - Cloud center using an organization's own servers in a platform-as-a-service (PaaS) or infrastructure-as-a-service (laaS) model. In this structure, the firewall application runs on the virtual servers and protects traffic going to, from, and between applications in the cloud. A firewall device or service that provides network traffic filtering and monitoring for virtual machines (VMs) in a virtualized environment. As Firewalls - Virtualized with a traditional network firewall, a virtual firewall inspects packets and uses security policy rules to block unapproved communication between virtual machines. Firmware is programming implanted in a hardware device's nonvolatile memory. Nonvolatile memory is a form of static random access memory whose contents are saved when a hardware device is turned off or loses its external power source. Firmware can function as either a Firmware standard operating environment a device's more complex software; or it may support less complex devices, acting as a complete operating system, performing all control, monitoring and data manipulation functions. An Internet of Things (IoT) gateway is a physical device or software program that serves as the connection point between the cloud and Gateway - Modular Internet-of-Things (IoT) controllers, sensors and intelligent devices. All data moving to the cloud, or vice versa, goes through the gateway, which can be either a dedicated hardware appliance or software program. reaith Management Information Systems (HMIS) Health Management Information Systems (HMIS) are one of the six building blocks essential for health system strengthening. HMIS is a data collection system specifically designed to support planning, management, and decision Health Management Systems - Network Connected making in health facilities and organizations. Elements may include: Hospitals, clinics, pharmacies, laboratories, billing, insurance providers, and health information exchanges in patient assessment, monitoring, and care delivery that are connected to an information network. These include networked equipment in diagnostic centers in hospital such as imaging (CAT Scan, MRI, other radiology); and in patient rooms (IV Health Systems/Devices - Network Connected pumps, patient monitors (temperature, blood pressure, oxygen level). An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as Industrial Control Systems - Networked distributed control systems and smaller control systems using programmable logic controllers to control localized processes. Source(s): NIST SP 800-53A Rev. 4

Microcontroller	A microcontroller (MCU for microcontroller unit, or UC for µ-controller) is a small computer on a single integrated circuit. It is similar to, but
	less sophisticated than, a system on a chip (SoC); an SoC may include a microcontroller as one of its components.
Internet Protocol Version 4 (IPV4)	Internet Protocol Version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP). An Internet Protocol address (IP address) is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication.
Internet Protocol Version 6 (IPV6)	Internet Protocol Version 6 (IPv6) provides more numerical addresses, simplifies network address assignments, and provides additional network security features. IPv6 utilizes 128-bit Internet addresses and supports 340,282,366,920,938,000,000,000,000,000,000,000,000,000,0
Intrusion Detection Systems (IDS) - Host Intrusion Detection (HIDS)	A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner. Source(s): NIST SP 800-82 Rev. 2
Intrusion Detection Systems (IDS) Network Intrusion Detection Systems (NIDS).	A program that monitors the characteristics of a single host and the events occurring within that host to identify and stop suspicious activity. Source(s): NIST SP 800-128
Mobile Device Operating Systems	The mobile operating system enables mobile device features and functions, including keypads, application synchronization, e-mail, thumbwheel and text messaging. Similar office computer products such as Windows, Linux, and Mac, the mobile operating system is simpler, utilizing fewer resources. It manages wireless functionality of local and broadband connections, multimedia and other electronic messaging.
Mobile Secure Gateways	Software or hardware appliances that provides secure communication between a mobile application and respective backend resources typically within a corporate network.
Network-Based Antivirus	Network-based antivirus looks at Internet traffic entering and leaving the campus network. If a virus is detected while a file is being downloaded, the download will be blocked before the malicious file reaches the computer.
Network Infrastructure Devices - Enterprise Level	Electronic devices linked to an enterprise-level communications backbone that connects computers and related devices across departments and workgroup networks, facilitating insight and data accessibility.
Network Intrusion Prevention Systems (NIPS)	A system that monitors a network and protects the confidentiality, integrity, and availability information flow across a network. Its main functions include protecting the network from threats, such as denial of service (DoS) and unauthorized usage. a combination of hardware and software systems that protect computer networks from unauthorized access and malicious activity.
Network Systems	Actions necessary to restore data files of an information system and computational capability after a system failure. Source(s): CNSSI 4009-2015
Networked Printers	A printer connected to a wired or wireless network. It may be Ethernet enabled and be cabled to an Ethernet switch, or it may connect to a Wi-Fi (wireless) network, or both.
Networked Scanners	Scanners come in hand-held, feed-in, and flatbed types and for scanning black-and-white only, or color. The device is networked when connected to a wired or wireless network, including Ethernet enabled and cabled to an Ethernet switch; or it may connect to a Wi-Fi (wireless) and the set of the se
Software Defined Networking (SDN)	Software-Defined Networking (SDN) is an architecture that decouples the network control and forwarding functions. Network intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch. SDN simplifies network design and operation because instructions are provided by SDN controllers instead of multiple, vendor-specific devices and protocols. Network control is directly programmable. Source: OpenNetworking.org
Software Publication Certificate	signature is a means for a software, application, or plug-in publisher to verify the authenticity of its own code when provided for download. It is a statement of authenticity, indicating that the download is actually from the source that it claims to be from and that the provider is
Supervisory Control and Data Acquisition (SCADA)-Networked	Reline it idnetities and approximate system that is capable or gathering and processing data and apprying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually characteristic transmission characteristic controls that must be used.
Technical Collaborations	Includes releated research acitivities, product design, development, joint ventures, shared testing, evaluation, and maintenance ativities, product-related data collection and analysis, shared trouble-shooting and service arrangements, etc.
Virtual Private Network (VPN)	Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.
Virtual Private Server (VPS)	Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line. Source(s): NIST SP 800-53 Rev. 4
Web proxies/content filtering	The process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users. Source(s): NIST SP 800-114
White List Program	The practice of specifying an index of approved software applications that are permitted to be present and active on a computer system. The goal of whitelisting is to protect computers and networks from potentially harmful applications. In general, a whitelist is an index of approved entities.
	BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

Pre	evious Page							<u>Next Page</u>
Se	ection: Organization Informati	on						
	Provide the following information for this or	ganization:						
	Facility/Organization Name							
	Street Address							
	City							
A.	State							
	Zip Code							
	Website							
	Phone Number							
_	Primary CAGE Code							
В.	Is your organization publicly traded or priva	tely held?	Private/Public	If your organization	is publicly trade	d, identify its	s stock ticker symbol.	
	Provide the following information for your p	arent organization(s), if applicab						
			Parent Organization	#1			Parent O	rganization #2
	Parent Name							
	Street Address							
	City State/Dravines							
	State/Province Country							
	Postal Code/Zip Code							
				If your parent organ	ization is public	ly traded id	entify its stock ticker	
C.	Is your parent organization publicly traded	or privately held?	Private/Public	symbol.		ly traded, lu	entity its stock licker	
	Provide the following identification codes, a	as applicable, for your organization						
	Data Universal Numbering System (DUNS) Code(s)		Harmonized Tariff Schedule (HTS) Code(s)				NAICS (6-digit) Code(s)	
D.	. (DON3) Code(s)		Code(s)					
	Find DUNS codes at: http://fedg	jov.dnb.com/webform	Find H	HTS codes at: http://ł	its.usitc.gov			nd NAICS codes at: nsus.gov/epcd/www/naics.html
	Indicate if your organization qualifies as an	y of the following types of busine	ess:					
	A small business enterprise (as defined by	the Small Business Administrati	on)				Yes/No	
E.							Yes/No	
E.	A historically underutilized business zone (I						Yes/No	
	A minority-owned business						Yes/No	
	A woman-owned business						Yes/No	
	A veteran-owned or service-disabled vetera	an owned business					Yes/No	
	Identify the government agencies to which	your organization sells information	on network-related har	dware and software	products, and as	sociated se	rvices:	
	Organization	Hardware	Software	Services				
	Department of Defense	Yes/No	Yes/No	Yes/No				
F.	Civilian U.S. Government Agencies							
	State Governments							
	Local Governments							
	Regional Government Organizations							
		BUSINESS CO	DNFIDENTIAL - Per S	ection 705(d) of the	Defense Produ	uction Act		
		D00111203 00		sector res(u) or the				

Section 1.a - Types of Information Network Products Designed, Manufactured and Outsourced

Instruction: Using drop-down responses accessed by clicking on the empty response cell, provide the requested information for each technology listed in the left column 1) Identify the specific types of network hardware and advance related products that your organization has <u>developed, manufactured, or marketed</u> since 2014; 2) Indicate those product lines for which your company markets related and columnation and advance and the second s

3) Identify the types of products that your organization sells where you employ or enlist third-party companies to perform servicing and upgrades;

hardware- and software-related products (models) that your organization has marketed/distributed since 2014; 5) Estimate the average in-service life of the specified hardware and software products; 6) Indicate withinere the enabling software code for your hardware and software products is written at company, contractor sites located in the United States, outside of the United States, or both.

Estimated Average In-Service Life of Software Products Before Replacement - Number of Years Written Use Third-Party Companies to Procure the Products that This Company Sells Use Third-Party Companies to Service and Upgrade Pro-ducts That This Company Sells Number of Estimated Average In-Service Life of Hardware Products Locations where Number of Marketed Enabling Product Software Code is Written Rebranded Products Made by Other Companies Distinct Distinct Types of Hardware/Software Technologies Developed Manufactured Marketed Before Replacement - Number of Years Hardware Software roducts oducts Company Sites In U.S. Company Sites In U.S. etwork Infrastructure Devices -100 scale 1-25 Drop-Down -100 scale 1-25 Drop-Down rdware dware ardware rdware dware rdware Company Sites Company Sites Routers oftware Software oftware Software oftware oftware Outside U.S. Outside U.S. Company Sites Company Sites In U.S. & Outside In U.S. & Outside witches oth Roth loth Both oth oth Contractor Sites Contractor Sites Gateways - Internet lone in U.S. lone None lone one one n U.S. Contractor Sites Contractor Sites Gateways - Internet Service Provider Grade Outside U.S. Outside U.S. Contractor Sites In & Contractor Sites In & Outside U.S. Gateways - Cloud Outside U.S. Gateway - Modular Internet-of-Things (IoT) Mobile Secure Gateways 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/Conent Filtering 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 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] Other Products Industrial Control Systems - Networked Supervisory Control and Data Acquisition (SCADA)-Networked Computer Operating Systems Computer Firmware Systems-On-Chip, Microcontroller 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) Comments: BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

4) State the number distinct



Section 1c - Types of U.S. Network Information Network Products Containing XYZ Hardware and Software AND Product and Services Collaboration and Development Activities With XYZ Companies

ostruction

1) Identify the specific types of information network hardware and software products that your organization has developed, manufactured, distributed or marketed since 2014 that incorporate or otherwise use any hardware, software, intellectual property or other technology sold by XYZ or its designated distributors and resellers. Use Comment boxes as necessary to describe company actions.

2) State whether any of the products or services listed in the left column that your company markets or sells:
 A) Are based on past or ongoing consulting or development collaborations with XY2; and
 B) Require XY2 hardware/software to operate; or whether the use of XY2 technologies in your organization's products is optional.
 3) State whether your organization has had since 2014 any kind of formal technology partnership program with XY2 or an XY2 affiliate.

	Act	ivities Involvin	g Network Produc	ts Utilizing XYZ	Hardware/Software Products a	nd Technologies	Identify All Ap	plicable Consulti Techr	ng and Developm nology	ent Activities by	Functional Dependency	Formal Relationship
Products Sold By Your Organization [Auto-Populate Column Elements from 1a - Block Out Non-Applicable Technologies]	Uses XYZ Products/ Technologies	Developed	Manufactured	Distributed	Marketed Under Your Organization's Name Rebranded Products Made by Other Companies	Use Third-Party Companies to Service and Upgrade Products the Company Sells Containing XYZ Technologies	Product <u>Consulting</u> Collaboration	Services <u>Consulting</u> Collaboration	Product <u>Development</u> Collaboration	Services <u>Development</u> Collaboration	Products/Services Sold that Require XYZ Technology to Operate; Use is Optional	Types of Formal Technology Partnerships/ Relationships with XY2 since 2014.
Network Infrastructure Devices	Yes/No	Hardware	Hardware	Hardware	Hardware	Hardware	Hardware	Hardware	Hardware	Hardware	Hardware	
Routers		Software	Software	Software	Software	Software	Software	Software	Software	Software	Software	Technology Partnership
Switches		Both	Both	Both	Both	Both	Both			Both	Both	Affiliate Program
Gateways - Internet		None	None	None	None	None	None	None	None	None	None	Whitelist Program
Gateways - Internet Service Provider Grade											Optional	Other
Gateways - Cloud												
Gateway - Modular Internet-of-Things (IoT)												
Mobile Secure Gateways												
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/Conent Filtering												
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												
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]												
Other Products												
Industrial Control Systems - Networked												
Supervisory Control and Data Acquisition (SCADA)-Networked												
Computer Operating Systems		-										
Computer Firmware			+									
Systems-On-Chip, Microcontroller 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		+	+									<u> </u>
Physical Access Control Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected	-	+	+	-								+
Telepresence Systems (Audio & Video Conferencing Systems)												+
Comments:		+	1									+
comments.		1			ITIAL - Per Section 705(d) of t		<u>.</u>		1	l	1	

Section 1.d - XYZ Technologies Deployed in Company Products & Terms of Technology License

Next Page

Instruction: 1) For each product type listed in the left column, identify all XYZ products and services (hardware and/or software- related) from which your company draws technology for inclusion in the hardware and software products that it markets. 2) For each product type listed in the left column, identify: the terms under which your company obtains license to use XYZ technologies. 3) Identify all of the XZY technologies listed below that your organization uses to support its internal business operations and

information networks. utilizes, identify whether it consists of a hardware or software product, service, or other type of good. 3) Identify all of the XZY technologies listed below that your organization uses to support its internal business operations and
 4) For each XYZ technology that your organization

	Applications of XYZ Technologies /Associated Intellectual Property in Your Company's Products	Single Technology Annual License Fee	Multi- Technology Annual License Fee	Single Technology Multi-Year License Fee	Multi-Year, Multi- Technology License Fee	One-Time Payment Permanent License	XYZ Technology Made Available for Free	Information Sharing Agreement	Your Company's Internal Business Operations and Network Systems	Products	Services	Other
Types of XYZ Product/Associated Intellectual Property												
XYZ Anti-Virus	Hardware	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Software	Software	Software
XYZ Internet Security	Software									Hardware	Hardware	Hardware
XYZ Total Security	Both									Both	Both	Both
XYZ Small Office Security	None									None	None	None
XYZ Professional Services												
XYZ Security Center												
XYZ Expert Services [Penetration, Application Security, Digital Forensics, Malware Analysis]												
Malware Analysis]												
XYZ Security Network												
XYZ Private Security Network												
XYZ Cyber Security Services [Security Education/Training]												
XYZ Industrial Cyber Security												
XYZ Cloud Security												
XYZ Hybrid Cloud Security												
XYZ Data Center Security												
XYZ Security for Storage [anti-virus]	-											
XYZ Whitelisting - Cloud Empowered												
XYZ Endpoint Security												
XYZ Endpoint Security for Business Select	-											
XYZ Endpoint Security for Business Advanced												
XYZ Endpoint Security - Cloud	-											
XYZ VirusDesk	-											
XYZ Mobile Security	-											_
XYZ Device Control												
XYZ Application Launch Control - Corporate Servers												
XYZ Application Control/Dynamic Whitelisting												
XYZ Endpoint Security												
XYZ Business Hub												
XYZ Password Manager												
XYZ Security for Windows 365												
XYZ Security for Virtualization - Agentless												
XYZ Security for Virtualization - Light Agent												
XYZ Security Virtual Machine												
XYZ Embedded Systems Security												
XYZ System Watcher [Anti-Ransom, Anti-Exploit]												
XYZ Security for Widows Server												
XYZ Web Control												
XYZ Distributed Denial of Service (DDOS)	-											
XYZ Maintenance Service Agreement	-											
XYZ Threat Intelligence	-											
XYZ Threat Management & Defense												
XYZ Automated Vulnerability Assessment	-											+
XYZ Automated Vulnerability Patch Management												
XYZ Multi-Layered Sensor Architecture												
XYZ Advanced Sandbox	-											
XYZ Analysis Engines												
XYZ HuMachine	-											
Other (Describe in Comment Box)												
Comments:												1

revious Page																																		_	Ne	ext Pag
Section 1.e - End Users of Hardware and Software P Instruction: For each of the business sectors shown in the top of the table												ld to th	om by	WOUL OF GO	ization																					
instruction. For each of the business sectors shown in the top of the table	e, identii	iy ule ty	pesori	mormau	onteci	mology p	Touters	Ontainin	ing arry Ar	12 tech	iologies so		iem by	your organ	nzation.	•																				e Devic
								В	usiness S	ectors														c	omputer	Operat	ting System	IS								erating
Business Sectors Purchasing Your Organization's Products that Contain XYZ Technologies and Operating Sytems Your Organization's Products Containing XYZ Technologies Can Run on -> ->	sumers mercial Business	dittes	scial Institutions	Oil Pipelines ufacturers	nications	tribution	re Facilities al Institutions	dia	tions	mmercial Airports	Ports J.S. Freight Railroads	Railroads	degional Transit Sys.	J.S. Govern. Agencies J.S. Armed Services	& Local ents	Sovernment	Armed	esearch ies	S	Hypervisor - VMWare ESX	r - erver	r - Microsoft		dows Server	10	7	swop	er	nux Workstation	nux Sever	yun on	-in			Svst	ems_
Types of XYZ Product/Associated Intellectual Property	Consumer	Electric Utilities	Financial I	Gas/ Oil Pipelin Manufacturers	Telecomunica	Water Distributi	Health Care Facil Educational Instit	News Media	Non-Profit Organizations Airlines	Commerci	Ports U.S. Freigl	Passenger Railroa	Regional 1	U.S. Govern. Ag U.S. Armed Sen	U.S. State & Loc Governments	Non-U.S. Gov	Non-U.S. Arm Services	Federal Research Laboratories BSD	Chrome OS	Hyperviso ESX	Hypervisor - Xen/XenServ	Hypervisor Hyper V	Mac OS	Windows	Windows 10	Windows	Older Windo Programs	Linux Server	Linux Wor	Red Hat Linux	Red Hat Linux Workstation	Unix Server	Unix	VMWorks	Android	iOS - Apple
. Network Infrastructure Devices																																				
Routers	Yes/NYes	s/NYes/1	VYes/N	Yes/ Yes/	/NYes/	NYes/NY	es/NYes,	NYes/N	Yes/NYes	s/NYes/	NYes/NYes	/NYes/	Yes/N	Yes/N Yes/I	VYes/No	Yes/N	Yes/No	Yes/NoYes	s/NYes/N	VYes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/NoY	es/NoY	'es/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/Nd	Yes/No	Yes/N
Switches					_							+																						\vdash	<u> </u>	—
Gateways - Internet Gateways - Internet Service Provider Grade	_	_			_			+ +		_		+ +							-														<u> </u>	\mapsto	<u> </u>	+
Gateways - Cloud	_	_			-							+							-	-												-		\vdash	<u> </u>	+
Gateway - Modular Internet-of-Things (IoT)		_			+			+ +				+							-							-						-		\vdash	<u> </u>	+
Mobile Secure Gateways		-			-		-	+		-		+			1				-	1	1	1										1	1	\vdash	<u> </u>	1
Network Security Devices																												_								
Antivirus Scanning Application - Host Based																																				
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)																																				
Firewalls - Host Based					_																													\vdash	<u> </u>	
Firewalls - Network Appliance	_				_	+						+			-				_													-	-	\vdash	<u> </u>	+
Firewalls - Cloud Firewalls - Virtualized	_	_			-				_										-	-												-		\vdash	<u> </u>	+
Web Application Firewalls	_	_			-														-													-		\vdash	<u> </u>	+
End Point Detection & Response (EDR)		-			+	-	_	+ +	-			+							-	-	-				-							-		\vdash	<u> </u>	+
Deep Packet Inspection (DPI) Appliance								+ +																											-	+
Security Information and Event Management (SIEM)		_			+		_	+ +				+							-						-							-			<u> </u>	+
Web Proxies/Conent Filtering								+ +																										\square		<u> </u>
Intrusion Detection/Prevention Systems																																				
Host Intrusion Detection (HIDS)																																				
Network Intrusion Detection Systems (NIDS)																																				
Host Intrusion Prevention Systems (HIPS)																																				-
Network Intrusion Prevention Systems (NIPS)																																				\square
Unified Threat Management (UTM) Systems																																				
Honeypot																																			(<u> </u>
Network Tar Pit Solutions								+ +																												<u> </u>
Data Loss Prevention (DLP)					-														-																	-
Data Recovery																																				
Network Systems																																				
Virtual Private Network (VPN)																																				
Virtual Private Server (VPS)																																		\square	<u> </u>	1
Virtualization Software - Bare Metal Hypervisor								+				+			-				_		 											-	I	\vdash	<u> </u>	+
Virtualization Software - Work Station-Based Hypervisor																																				
Software Defined Networking (SDN) solutions																																				
Other [Define in Comment Box]																																			L	
Other Products																																				
Industrial Control Systems - Networked		-				+		+		_		+			-				_													-	l	\vdash	 	+
Supervisory Control and Data Acquisition (SCADA)-Networked		_			-			+		_		+			+				_		<u> </u>											-	l	\vdash	<u> </u>	
Computer Operating Systems Computer Firmware		-	+	\vdash	-	+		+			+	+			 			\vdash			+											-	I	\vdash	<u> </u>	+
Systems-On-Chip, Microcontroller Devices		+			+	+ +		+ +			+	+			+			\vdash	-	-	+	+										-	-	\vdash	<u> </u>	+
Mobile Device Operating Systems		-			-										1				-	1	1					-						1	1	\vdash	(<u> </u>
Multi-Function Devices - Printers-Copiers-Scanners					-							+			1				-		1	1				-						1		\rightarrow		-
Networked Printers																																				
Networked Scanners															1						1	1										1		\square		
Health Management Systems - Network Connected																																				
Health Systems/Devices - Network Connected																																				
Physical Access Control Systems - Network Connected																												_								
Physical Security Video Monitoring Systems - Network Connected																					1													\square	<u> </u>	
Telepresence Systems (Audio & Video Conferencing Systems)					_	+					+	+							_		+											-	-	\mapsto	<u> </u>	+
Comments:																					L														<u> </u>	
										BUSINE	SS CONFIE	ENTIAL	L - Per	Section 70	5(d) of t	the Def	fense P	roduction /	Act																	

evious Page									Next F
Section 1.f - Modes of Accessing XYZ Technologies Instruction: 1) For each product type listed in the left column, identify t									manufactures.
listed in the left column that was sold by your organization from 2014-2						egrated into the p	roudets that your eo	2) F	or each product ty
3) State whether any of the cloned/counterfeit products utilize your co					uon.				
	1	1	1	i			Ì	İ	1
	De de cal California	Deduced		Software Installed	Software Installed at				
	Packaged Software Purchased Directly	Software Sold by	Packaged Software Downloaded	at Your Company's Product	Your Product Manufacturing	Cloned/ Counterfeit	Cloned/ Counterfeits	Cloned/ Counterfeit	Cloned/ Counterfei
[Auto-Populate from 1c]	from XYZ Installed by Your	XYZ Authorized Third-Party	Directly from	Manufacturing	Facilities by XYZ-	Hardware	Contain XYZ	Software	Contain XY
	Company's Staff	Reseller	XYZ Servers	Facilities by XYZ Employees	Authorized Third- Party Firms	Products	Technology	Products	Technolog
Network Infrastructure Devices	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No
Routers							Not Known		Not Known
Switches									-
Gateways - Internet									
Gateways - Internet Service Provider Grade Gateways - Cloud									-
Gateways - Cloud Gateway - Modular Internet-of-Things (IoT)									
Mobile Secure Gateways									
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/Conent Filtering									
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									
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] Other Products									
Other Products Industrial Control Systems - Networked									
Supervisory Control and Data Acquisition (SCADA)-Networked									
Computer Operating Systems				1			1	1	
Computer Firmware									
Systems-On-Chip, Microcontroller 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) Comments:				+				+	+
comments:			L	l) of the Defense Pr			1	L	<u> </u>

Reasons for Using XYZ Technology -> -> -> Types of XYZ Product/Associated Intellectual Property Z Anti-Virus Z Internet Security Z Total Security Z Total Security Z Total Security Z Small Office Security Z Forfessional Services Z Security Center Z Expert Services enetration, Application Security, Digital Forensics, Malware Analysis] Z Security Network Z Security Network Z Cyber Security Network Z Cyber Security Network Z Cyber Security Services [Security Education/Training] Z Industrial Cyber Security Z Cloud Security Z Hybrid Cloud Security	Lowest Pricing	Performance/ Effectiveness	Reliability	Integration Time / Latency	Technical Support	Technical Collaborations	Tech. Superiority	No Competitive Equivalent	Accessibility of Technologies	Contract Terms	Financing	XYZ Financial Rebates	Offers Full-Service Network Security Manage. Services	Other Comment Box)	Other
Z Anti-Virus Z Internet Security Z Total Security Z Total Security Z Small Office Security Z Professional Services Z Security Center Z Expert Services enetration, Application Security, Digital Forensics, Malware Analysis] Z Security Network Z Security Network Z Security Network Z Cyber Security Network Z Cyber Security Network Z Cyber Security Services [Security Education/Training] Z Industrial Cyber Security Z Cloud Security Z Hybrid Cloud Security												×	Offers Netw. Mana	(Use Co	[Explain in Comment Box Below]
Z Internet Security Z Total Security Z Small Office Security Z Professional Services Z Security Center Z Expert Services enetration, Application Security, Digital Forensics, Malware Analysis] Z Security Network Z Security Network Z Private Security Network Z Cyber Security Network Z Cyber Security Services [Security Education/Training] Z Industrial Cyber Security Z Cloud Security Z Hybrid Cloud Security															
Z Total Security Z Small Office Security Z Professional Services Z Security Center Z Expert Services enetration, Application Security, Digital Forensics, Malware Analysis] Z Security Network Z Security Network Z Private Security Network Z Cyber Security Network Z Cyber Security Services [Security Education/Training] Z Industrial Cyber Security Z Cloud Security Z Hybrid Cloud Security															
Z Small Office Security Z Professional Services Z Security Center Z Expert Services Expert Services S Security Network Z Security Network Z Cyber Security Network Z Cyber Security Services [Security Education/Training] Z Industrial Cyber Security Z Cloud Security Z Hybrid Cloud Security					1										
Z Professional Services Z Security Center Z Expert Services enetration, Application Security, Digital Forensics, Malware Analysis] Z Security Network Z Private Security Network Z Cyber Security Services [Security Education/Training] Z Industrial Cyber Security Z Cloud Security Z Hybrid Cloud Security															
Z Security Center Z Expert Services enetration, Application Security, Digital Forensics, Malware Analysis] Z Security Network Z Private Security Network Z Cyber Security Services [Security Education/Training] Z Industrial Cyber Security Z Cloud Security Z Hybrid Cloud Security			1												
Z Expert Services enetration, Application Security, Digital Forensics, Malware Analysis] Z Security Network Z Private Security Network Z Cyber Security Services [Security Education/Training] Z Industrial Cyber Security Z Cloud Security Z Hybrid Cloud Security															
enetration, Application Security, Digital Forensics, Malware Analysis] Z Security Network Z Private Security Network Z Cyber Security Services [Security Education/Training] Z Industrial Cyber Security Z Cloud Security Z Hybrid Cloud Security															
Z Private Security Network Z Cyber Security Services [Security Education/Training] Z Industrial Cyber Security Z Cloud Security Z Hybrid Cloud Security															
Z Cyber Security Services [Security Education/Training] Z Industrial Cyber Security Z Cloud Security Z Hybrid Cloud Security															
Z Industrial Cyber Security Z Cloud Security Z Hybrid Cloud Security															
Z Cloud Security Z Hybrid Cloud Security															
Z Hybrid Cloud Security															
Z Data Center Security															
Z Security for Storage [anti-virus]															
Z Whitelisting - Cloud Empowered															
Z Endpoint Security															
Z Endpoint Security for Business Select															
Z Endpoint Security for Business Advanced															
Z Endpoint Security - Cloud Z VirusDesk															
Z Mobile Security															
Z Device Control Z Application Launch Control - Corporate Servers															
Z Application Control/Dynamic Whitelisting Z Endpoint Security															
Z Business Hub															
Z Password Manager															
Z Security for Windows 365															
Z Security for Virtualization - Agentless															
Z Security for Virtualization - Light Agent					-										
Z Security Virtual Machine															
Z Embedded Systems Security															
Z System Watcher [Anti-Ransom, Anti-Exploit]															
Z Security for Widows Server															
Z Web Control			<u> </u>												
Z Distributed Denial of Service (DDOS)															
Z Maintenance Service Agreement Z Threat Intelligence			-												
Z Inreat Intelligence Z Threat Management & Defense															
Z Inreat Management & Defense Z Automated Vulnerability Assessment															
Z Automated Vulnerability Assessment Z Automated Vulnerability Patch Management															
Z Automated Vulnerability Patch Management Z Multi-Layered Sensor Architecture			-		-										
Z Multi-Layered Sensor Architecture					-										
Z Analysis Engines Z HuMachine															
her (Describe in Comment Box)			-												
mments:															

nstruction: Identify all information network hardware and software sold by lown under the "Product Supported by XYZ" column. Select "None" for h	your company since 2	2014 that incorporat	es or otherwise o	ontains embedded	XYZ technologies by selecting a response from the dr
lown under the "Product Supported by XYZ" column. Select "None" for h ontaining XYZ technologies.	ardware products sold	by your company t	hat do not contair	NYZ technologies	. Provide verson numbers for each model reported as
nter all additional product names and model numbers. Information on add	litional product model	numbers may be e	ntered in successi	ve form blocks tha	t are reached by scrolling this page to the right $\hfill \hfill
	Inte	egration of XYZ Tec	nnologies in Infor	mation Technolog	y Products - Technology Type/Versions
Hardware/Software Products Sold By Your Organization that Contain XYZ Technology [Auto-Populate This List Below from 1c]	Product Name #1	#1 Your Company's Product Series/Model Number	Product Supported by XYZ Technology By Type	Supporting XYZ Version Numbers (if applicable)	Comments
Network Infrastructure Devices			Hardware		
Routers			Software		
witches			Both		
Gateways - Internet			None		
Gateways - Internet Service Provider Grade					
Gateways - Cloud					
Sateway - Modular Internet-of-Things (IoT)					
Nobile Secure Gateways					
Network Security Devices					
Antivirus Scanning Application - Host Based Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)					
irewalls - Host Based					
irewalls - Network Appliance		1			
irewalls - Cloud					
irewalls - Virtualized					
Veb Application Firewalls					
nd Point Detection & Response (EDR)					
Deep Packet Inspection (DPI) Appliance					
ecurity Information and Event Management (SIEM)					
Veb Proxies/Conent Filtering					
ntrusion Detection/Prevention Systems					
lost Intrusion Detection (HIDS)					
Network Intrusion Detection Systems (NIDS)					
lost Intrusion Prevention Systems (HIPS)					
Network Intrusion Prevention Systems (NIPS)					
Jnified Threat Management (UTM) Systems					
loneypot					
Network Tar Pit Solutions					
Data Loss Prevention (DLP)					
Data Recovery Vetwork Systems					
/irtual Private Network (VPN)					
/irtual Private Server (VPS)					
/irtualization Software - Bare Metal Hypervisor					
/irtualization Software - Work Station-Based Hypervisor					
oftware Defined Networking (SDN) solutions					
Other [Define in Comment Box]					
Other Products					
ndustrial Control Systems - Networked					
upervisory Control and Data Acquisition (SCADA)-Networked					
Computer Operating Systems					
Computer Firmware					
systems-On-Chip, Microcontroller Devices					
Abile Device Operating Systems					
Aulti-Function Devices - Printers-Copiers-Scanners					
Networked Printers					
Vetworked Scanners					
Health Management Systems - Network Connected		+	+		
Iealth Systems/Devices - Network Connected Physical Access Control Systems - Network Connected					
Physical Access Control Systems - Network Connected			-		
elepresence Systems (Audio & Video Conferencing Systems)					
			1		

Next Page

Previous Page

Section 2.b - Integration/Embedding of XYZ Software into Domestic Manufacturers Information Technology Products

For each type of information technology product (hardware or software) identified on the previous page as incorporating or otherwise containing any XYZ technologies: 1) provide XYZ product model numbers 2) state the functions and capabilities of the XYZ software; 3) specify the methods used for integrating XYZ technologies into your organization's products.

Enter all additional product model numbers. Information on additional product model numbers may be entered in form blocks reached by scrolling this page to the right 🛙 🖇

-		Des	cripti	on of)	(YZ Te	chnolog	ies in	Inform	nation	Technol	ogy Products - Functions &	Capabilities/Integration Methods
							~	-	_			
		#1 Your Company's Product Series/Model Number	Local Anti-Virus	Cloud Anti-Virus	E-mail Scanning	Identify Theft Scanning	IP Loss Preventior	Network Intrusion Detect.	Network Firewall	Other (Use Comment Box)	Description of Methods for Integrating XYZ Technology into Your Company's Products	Comments
А.	Network Infrastructure Devices	Auto-Populate										
	Routers										Compiled Separately	
	Switches										Compiled Together	
	Gateways - Internet										Transformed	
	Gateways - Internet Service Provider Grade										Executed	
	Gateways - Cloud										Other (Use Comment Box)	
	Gateway - Modular Internet-of-Things (IoT)											
	Mobile Secure Gateways											
В.	Network Security Devices											
	Antivirus Scanning Application - Host Based											
	Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)											
	Firewalls - Host Based							<u> </u>	<u> </u>			
	Firewalls - Network Appliance Firewalls - Cloud											
	Firewalls - Cloud											
	Web Application Firewalls											
	End Point Detection & Response (EDR)		-									
	Deep Packet Inspection (DPI) Appliance											
	Security Information and Event Management (SIEM)											
	Web proxies/content filtering											
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											
D.	Network Systems											
	Virtual Private Network (VPN)											
-	Virtual Private Server (VPS) Virtualization Software - Bare Metal Hypervisor								<u> </u>			
-	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											
	Mobile Device Operating Systems											
	Multi-Function Devices - Printers-Copiers-Scanners											
	Networked Printers											
	Networked Scanners											
	Health Management Systems - Network Connected								<u> </u>			
	Health Systems/Devices - Network Connected											
	Physical Access Control Systems - Network Connected											
	Physical Security Video Monitoring Systems - Network Connected Telepresence Systems (Audio & Video Conferencing Systems)											
	Comments:											
		SINESS CONFIDENTIA	I - Po	r Sart	ion 7	05(d) ~	fthe	Defer	se Pro	duction	Act	1
L	BU	SINESS CONFIDENTIA	гt	, JECI	.0117	Ju) 0		Dei Cili	JC 110	ฉนะแป	1 7004	

rov	ious Page				Next
	tion 2.c - Integration/Embedding of XYZ Software int	o Manufacturers	'Information Te	chnology Products	
ec	lion 2.c - Integration/Embedding of X12 Software int	omanulacturers	mormation re	chilology Products	
	For the different information network products identified on the previous	page as incorporating of	or otherwise containing	embedded XYZ technolog	gies, provide:
	 applicable model numbers; associated application program interfaces (APIs); and 				
	 the software publication certificate associated with XYZ technologies be 	eing integrated into you	r organization's produc	ts.	
	Enter all additional product model numbers. Information on additional pr	oduct model numbers r	nav be entered in form	blocks reached by scrollin	g this page to the right 0 0
		Integration of XYZ	Software and Service	s in Information Technolo Publication Certificates	gy Systems - Program Interfaces/Softwa
	Hardware/Software Products Sold By Your Organization that Contain	#1 Your Company's Product	Associated Application	Method for Signing Software	Commente
	XYZ Technology	Series/Model Number	Program Interfaces (APIs)	Publication Certificate	Comments
			Interfaces (APIS)	Certificate	
	Network Infrastructure Devices	Auto Populate	Dinalina	Co Cienad	
	Routers		Pipeline Rest	Co-Signed	
	Switches		Shared Memory	Signed Shared Key	
	Gateways - Internet	-	Soap	Not Signed	
	Gateways - Internet Service Provider Grade Gateways - Cloud		Other (Use Comment Box)	None	
	Gateway - Modular Internet-of-Things (IoT)		Other (ose commencedox)	Other (Use Comment Box)	
	Mobile Secure Gateways				
	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/Conent Filtering				
	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				
	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]				
	Other Products				
	Industrial Control Systems - Networked				
	Supervisory Control and Data Acquisition (SCADA)-Networked				
	Computer Operating Systems				
	Computer Firmware				
	Systems-On-Chip, Microcontroller 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)				
	Comments:				

us Page				Next Pa
on 2.d - Integration/Embedding of XYZ Software	into Manufactu	rers' Information Technol	ogy Products	
	ous page as incorpora	ting or otherwise containing embedde	ed XYZ technologies, provide:	
) Levels of system access enabled by XYZ software;				
	al product model num	bers may be entered in form blocks re	eached by scrolling this page to	the right 🛛 🖛
	Integration of XY	Z Software and Services in Information	on Technology Systems - Syste	m Access & Types of Data
	#1 Your			
By Your Organization that Contain	Company's Product Series/Model			Comment
ATZ Technology	Number		, ,	
Network Infrastructure Devices	Auto-Populate			
Routers		System Configuration	Operating Sys. Data	
iwitches		Prop. Busn. Data	Application Data	
Gateways - Internet		System Customization Data	User Data	
Gateways - Internet Service Provider Grade		Application Customization Data	Other (Use Comment Box)	
Sateways - Cloud		Other (Use Comment Box)		
Mobile Secure Gateways				
Veb Application Firewalls				
nd Point Detection & Response (EDR)				
Deep Packet Inspection (DPI) Appliance				
Security Information and Event Management (SIEM)				
Inified Threat Management (UTM) Systems				
loneypot				
Network Tar Pit solutions				
Data Loss Prevention (DLP)				
Data Recovery				
Network Systems				
/irtual Private Network (VPN)				
/irtual Private Server (VPS)				
/irtualization Software - Bare Metal Hypervisor				
•				
Physical Access Control Systems - Network Connected				
Neurisel Consults Mideo Manitorius Contenes - Materiali Comparted				
'nysical security video Monitoring Systems - Network Connected				
Physical Security Video Monitoring Systems - Network Connected				
relepresence Systems (Audio & Video Conferencing Systems)				
	on 2.d - Integration/Embedding of XYZ Software ior the types information technology products identified on the previ) Model numbers;) Levels of system accesse enabled by XYZ software;) Types of data that can be accessed. Enter all additional product model numbers. Information on addition By Your Organization that Contain XYZ Technology Vetwork Infrastructure Devices touters witches Jateways - Internet Service Provider Grade Jateways - Internet Service (DP) Appliance Jateways - Service Jateways - Based Jateways - Internet Grade Jateways - Intrusion Detection (HDS) Jata Loss Prevention Systems (NIDS) Jata Loss Prevention Systems (NIDS) Jata Loss Prevention Glupp Jata Loss Prevention Glupp Jata Recovery <u>Jetwork Intrusion Detection Systems (NIDS)</u> Jata Loss Prevention Glupp Jata Recovery <u>Jetwork Staton - Based Hypervisor</u> Jirtual Private Server (VPS) Jirtual Jata Network (VPN) Jirtual Private Server (VPS) Jirtual Jata Netework Kytewas Joher Products Joher Products Joher Products Joh	on 2.d - Integration/Embedding of XYZ Software into Manufactu in ded numbers; i) Model numbers; i) Vess of system access enabled by XYZ software; i) Types of data that can be accessed. Enter all additional product model numbers. Information on additional product model numbers, information on additional product model numbers. Integration of XY By Your Organization that Contain XYZ Technology fi 1 Your Company's Product Sold Number Integration of XY Vetwork Infrastructure Devices Auto-Populate touters integration of XY Steways - Internet Stateways - Internet Service Provider Grade Steways - Cloudiar Internet-of-Things (IOT) internet Service Provider Grade Steways - Cloudiar Internet-of-Things (IOT) intivirus Scanning Appliance Firewalls - Network Appliance internet Service Provider Grade Internet Service Provider Grade intivirus Scanning Appliance Firewalls - Network Appliance internet Service Provider Grade Deep Packet Inspection (PDI Appliance intro Security Devices Ind Point Detection Firewalls intro Security Devices Ind Point Detection Firewalls intro Secure	on 2.d - Integration/Embedding of XYZ Software into Manufacturers' Information Technology or between information technology products identified on the previous page as incorporating or otherwise containing embedding of system access enabled by XYZ software; I brees of as that can be accessed. Integration of XYZ software information on additional product model numbers may be entered in form blocks or information that Contain XYZ Technology Integration of XYZ software and Services in Information XYZ software and Services in Information XYZ Technology Vetwork Infrastructure Devices Auto Populate System Configuration that Contain XYZ Technology Vetwork Infrastructure Devices Auto Populate System Configuration Proceeding System Configuratis Proceeding System Configuratis Proceeding System System System S	an 2.d - Integration/Embedding of XVZ Software into Manufacturers' Information Technology Products is the production behavious products identified on the previous page as incorporating or otherwise containing embedded XVZ technologies, provide: it hold numbers: Integrated and additional product model numbers information additional product model numbers may be entered in form blocks reached by strolling this page to it and the product model numbers. Information additional product model numbers may be entered in form blocks reached by strolling this page to it and the product model numbers. Information additional product model numbers may be entered in form blocks reached by strolling this page to it and the product model numbers. Information additional product model numbers may be entered in form blocks reached by strolling this page to it and the product model numbers. Information additional product model numbers may be entered in form blocks reached by strolling this page to it and the product model numbers. Information additional product model numbers may be entered in formation. Technology Systems - System is a stroke information between additional product model numbers may be entered in formation. Technology Systems - System is a stroke information between additional product model numbers may be entered in formation. Technology Systems - System is a stroke information between additional product model numbers may be entered in formation. Technology Systems - System is a stroke information additional product model numbers may be entered in formation. Technology Systems - System is a stroke information additional product model numbers may be entered in formation. Technology Systems - System is a stroke information additional product model numbers may be entered in formation. Technology Systems - System is a stroke information additional product model numbers may be entered in formation. Technology Systems - System is a stroke information additional product model numbers may be entered in formation. Technology

Section 2.e - Integration/Embedding of XYZ Software into Manufacturers' Information Technology Products

Instruction: 1) Identify the conditions under which XYZ software can perform its functions; and 2) Specify the measures invoked by your organization to limit XYZ software and services from the balance of the identified product.

Enter all additional product model numbers. Information on additional product model numbers may be entered in form blocks reached by scrolling this page to the right 🛽 🖛

Integration of XYZ Software and Services in Software Systems - Functional Conditions for XYZ Software/Limits on XYZ in Systems

		#1 Your Company's Product Series/Model Number	Methods by Which XYZ Technology Can Perform Its Functions	Measures Invoked to Isolate XYZ Software & Services from Rest of System	Comments
A.	Network Infrastructure Devices	Auto-Populate			
	Routers		Internet Access	Network Isolation	
	Switches		Oper. Sys. Policy Limits	Library Configuration	
	Gateways - Internet		Blocked Functions	CPU Demand Limits	
	Gateways - Internet Service Provider Grade	-	Code Modification	Other (Use Comment Box)	
	Gateways - Cloud		User Level Application	o thor (ose comment box)	
	Gateway's cloud Gateway - Modular Internet-of-Things (IoT)		System Services		
			Other (Use Comment Box)		
D	Mobile Secure Gateways Network Security Devices		Certer (ose connicit box)		
ь.	Antivirus Scanning Application - Host Based				
	Antivirus Scanning Application Trost 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/Conent Filtering				
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)	-			
D.	Data Recovery				
D.	Network Systems Virtual Private Network (VPN)				
	Virtual Private Server (VPS)				
	Virtualization Software - Bare Metal Hypervisor				
	Virtualization Software - Bare Metal 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				
	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)				
	Comments:				

Section 2.f - Product Design, Manufacturing, and Servicing of Products Containing XYZ Technologies - Internal-External/Third Party Services

Instruction: For the information technology products are designed internally by company staff, externally by contractors, or by both company employees and external contractors; 1) Indicate whether your company's products are designed internally by company staff, externally by contractors, or by both company employees and external contractors; 2) State the types of products for which your company formally designates third-party companies as "Manufacturer Authorized" to service and upgrade the products for which the third-party companies authorized to service and upgrade the products for which the third-party companies authorized to service and upgrade the products that your company sells. 3) Provide the names of the third-party companies authorized to service and upgrade the products that your company sells. Enter all additional product model numbers. Information on additional product model numbers may be entered in form blocks reached by scrolling this page to the right 0 0 0

Next Page

Production Private Construct Interfact		Integrat	tion of XYZ S	Software, Hard	dware, & Services in	Hardware Systems - Product Design, Service and Upgrade Practices
NuclearNuclearNuclearNuclearNuclearSubtesSoftwareSoftwareSoftwareGalaways. InternetNoneNoneNoneGalaways. InternetNoneNoneNoneGalaways. Subtes/Internet of Thegi (Internet		Company's Product Series/Model	Internal Design	Outsourced Design	Companies to Service and Upgrade products	Party Organizations that Service and Upgrade Your
junctionjork/arejork/arejork/areGateways-internet Service Prode GadeNoneNoneGateways-internet Service Prode GadeNoneNoneGateways-Vodular Internet of Thing [07]NoneNoneGateways-Vodular Internet of Thing [07]NoneNoneGateways-Vodular Internet of Thing [07]NoneNoneMobile Secure GatewaysNoneNoneNone Security DeviceNoneNoneNone Security DeviceNoneNoneNone Security DeviceNoneNoneNone Security DeviceNoneNonePrevalls-Note Security DeviceNoneNoneNone Se	A. Network Infrastructure Devices	Auto-Populate				
ServerServerNorthNorthNorthNorthNorthCalaway, -Stadiu Internet -Ting ServerCalaway, -Stadiu Internet -Ting ServerCalaway, -Stadiu Internet -Ting ServerCalaway, -Stadiu Internet -Ting ServerCalaway, -Stadiu Internet -Ting ServerMobio Scare Calaway -Stadiu Internet -Ting ServerCalaway, -Stadiu Internet -Ting ServerCalaway, -Stadiu Internet -Ting ServerMobio Scare Calaway - Stadiu Internet - Ting ServerCalaway, -Stadiu Internet - Ting ServerCalaway, -Stadiu Internet - Ting ServerMobio Scare Calaway - Stadiu Internet - Ting ServerCalaway, -Stadiu Internet - Ting ServerCalaway, -Stadiu Internet - Ting ServerMobio Scare Calaway - Stadiu Internet - Stadiu Inter	Routers		Hardware	Hardware	Hardware	
Secury - Monie Service Provides GadeNoneNoneNoneGateway - Monie Internet of Hings [01]IIIIMalli Scourt Gateway - Monie Scouthy DeviseIIIIMalli Scourt Gateway - Monie Scouthy DeviseIIIIMalli Scourt Gateway - Monie Scouthy DeviseIIIIMather Scanning Applicater - Instance Boardary (Gateway-base)IIIIPrevals - Note StandIIIIIPrevals - Note StandIIIIIStand Prevals - Note StandIIIIINote Stand PrevalsIIIIIINote Stand PrevalsIIIIIINote Stand PrevalsIIIIIIStand PrevalsIIIIIINote Stand PrevalsIIIIIINote Stand PrevalsIIIIIIStand PrevalsIII <t< td=""><td>Switches</td><td></td><td>Software</td><td>Software</td><td>Software</td><td></td></t<>	Switches		Software	Software	Software	
Genergy - CouldCould Could Co	Gateways - Internet		Both	Both	Both	
SetureSetureSetureSeture8. Network Security DeviceII8. Network Security DeviceII8. Network Security DeviceIIArthritus Scanning Appliance - Instander (Gateway-based)IIFirewalls - Network ApplianceIIFirewalls - Network ApplianceIIFirewalls - Network ApplianceIIFirewalls - Network ApplianceIIFirewalls - Network ApplianceIICose pack Improvement (DR)IICose pack Improvement (DR)IISecurity Information and Cvert Management (SIM)IINetwork Network InfolioIISecurity Information and Systems (NDS)IINethor Network InfolioIINetwork Intradion Detection Systems (NDS)IINetwork Intradion Detection Systems (NDS)IINetwork Intradion Network InfolioIINetwork Intradion Network InfolioII <td>Gateways - Internet Service Provider Grade</td> <td></td> <td>None</td> <td>None</td> <td>None</td> <td></td>	Gateways - Internet Service Provider Grade		None	None	None	
Media Scare CalewaysIIMethods Scare CalewaysIIArbitris Scarning Applicators - Inclus BandIIArbitris Scarning Applicators - Inclus BandIIFexalls - Hots BasedIIFexalls - Nather KaplianceIIFexalls - Nather KaplianceIIBack Inspector (DN) ApplianceIIBack Inspector (DN) ApplianceIIBack Inspector (DN) ApplianceIIMusica Cater Marce (Natio)IIHostin Cater Marce (Natio)IIHostin Intruion Prevention SystemIIHostin Intruion Prevention Systems (NPS)IIHostin Intruion Prevention Systems (NPS)II	Gateways - Cloud					
a)Network Scarching Agailance - Network Regulation - Value BasedImage: Scarching Agailance - Schreiber Basedary (Catrowy-based)Prevails - Network Regulance - Instruct Basedary (Catrowy-based)Image: Schreiber Basedary (Catrowy-based)Prevails - Network Regulance - Instruct Basedary (Catrowy-based)Image: Schreiber Basedary (Catrowy-based)Prevails - Network Regulance - Instruct Basedary (Catrowy-based)Image: Schreiber Basedary (Catrowy-based)Prevails - CodaImage: Schreiber Basedary (Catrowy-based)Image: Schreiber Basedary (Catrowy-Basedary (Cat	Gateway - Modular Internet-of-Things (IoT)					
Arking Saming Applicate - Host Bandary (Gatway-based) Image: Sami applicate - Entropy Bandary (Gatway-based) Freezils - Host Band Image: Sami applicate - Entropy Bandary (Gatway-based) Freezils - Host Applicate - Entropy Bandary (Gatway-based) Image: Sami applicate - Entropy Bandary (Gatway-based) Freezils - Host Applicate Image: Sami applicate - Entropy Bandary (Gatway-based) Freezils -	Mobile Secure Gateways					
Arbina Saming Appliance - Exclave Boundary (Gateway-based) Image: Saming Appliance - Exclave Boundary (Gateway-based) Frewails - Network Appliance Image: Saming Appliance - Exclave Boundary (Gateway-based) Frewails - Coold Image: Saming Appliance - Exclave Boundary (Gateway-based) Frewails - Coold Image: Saming Appliance - Exclave Boundary (Gateway-based) End Patie Detection Response (EDR) Image: Saming Appliance - Exclave Boundary (Gateway-based) Deep Patie Interction Response (EDR) Image: Saming Appliance - Exclave Boundary (Gateway-based) Security Information and Exerct Management (SHA) Image: Saming Appliance - Exerct Management (SHA) Verb ProstConcent Filtering Image: Saming Appliance - Exerct Management (SHA) Verb ProstConcent Filtering Image: Saming Appliance - Exerct Management (SHA) Verb ProstConcent Filtering Image: Saming Appliance - Exerct Management (SHA) Verb ProstConcent Filtering Image: Saming Appliance - Exerct Management (SHA) Verb ProstConcent Filtering Image: Saming Appliance - Exerct Management (SHA) Verb ProstConcent Management (SHA) Image: Saming Appliance - Exerct Management (SHA) Verb ProstConcent Management (SHA) Image: Saming Appliance - Exerct Management (SHA) Verb ProstConcent Management (SHA) Image: Saming Appliance - Exerct Management (SHA) Verb ProstConcent Management (SHA) Image: Saming Appliance - Exerct Management (SHA)	3. Network Security Devices					
iPrevails House Applance Image: Applance iPrevails Image: Applance Image: Applance iPrevails Image: Applance Image: Applance Security Information and Event Management (SIRM) Image: Applance Image: Applance Security Information and Event Management (SIRM) Image: Applance Image: Applance Security Information and Event Management (SIRM) Image: Applance Image: Applance Security Information and Event Management (SIRM) Image: Applance Image: Applance Image: Applance Image: Applance Image: Applance Security Information and Event Management (SIRM) Image: Applance Image: Applance Image: Applance Image: Applance <td>Antivirus Scanning Application - Host Based</td> <td></td> <td></td> <td></td> <td></td> <td></td>	Antivirus Scanning Application - Host Based					
Freewils - Network ApplanceImage: Network ApplanceImage: Network ApplanceFreewils - CouldImage: Network ApplanceImage: Network ApplanceWeb Applance FreewilsImage: Network ApplanceImage: Network ApplanceScarlt Information and Level Management (SEM)Image: Network ApplanceImage: Network ApplanceWeb Applance Detection SystemsImage: Network ApplanceImage: Network ApplanceWeb Applance Detection SystemsImage: Network ApplanceImage: Network ApplanceWeb Applance Detection Systems Network ApplanceImage: Network ApplanceImage: Network ApplanceNetwork IntraJon Detection Systems NetworkImage: Network ApplanceImage: Network ApplanceNetwork IntraJon Detection Systems NetworkImage: Network ApplanceImage: Network ApplanceNetwork Tar Network IntraJon Detection Systems NetworkImage: Network ApplanceImage: Network ApplanceNetwork Tar Network IntraJon Detection Systems NetworkImage: Network IntraJon Detection SystemsImage: Network IntraJon Detection SystemsNetwork Tar Network IntraJon Detection SystemsImage: Network IntraJon Detection SystemsImage: Network IntraJon Detection SystemsNetwork Tar Network IntraJon Detection SystemsImage: Network IntraJon Detection SystemsImage: Network IntraJon Detection SystemsNetwork Tar Network IntraJon Detection SystemsImage: Network IntraJon Detection SystemsImage: Network IntraJon Detection SystemsNetwork Tar Network IntraJon Detection SystemsImage: Network IntraJon Detection SystemsImage: Network IntraJon Detection SystemsNetwork Tar Network IntraJon	Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)					
Freewis Image: Court of the section	Firewalls - Host Based					
iFixedia Image: Setting	Firewalls - Network Appliance					
Web Application TirewallsImage and the set of the se	Firewalls - Cloud					
End Aniz Detection A Besopries (EDR) Image and the Management (SIEM) Image and the Management (SIEM) Deep Packet Inservers Management (SIEM) Image and the Management (SIEM) Image and the Management (SIEM) Web Produce' Contert Filtering Image and the Management (SIEM) Image and the Management (SIEM) Met Infrusion Detection Systems (MIDS) Image and the Management (SIEM) Image and the Management (SIEM) Met Infrusion Detection Systems (MIDS) Image and the Management (SIEM) Image and the Management (SIEM) Metwork Infrusion Detection Systems (MIDS) Image and the Management (SIEM) Image and the Management (SIEM) Metwork Infrusion Detection Systems (MIDS) Image and the Management (SIEM) Image and the Management (SIEM) Metwork Infrusion Detection Systems (MIDS) Image and the Management (SIEM) Image and the Management (SIEM) Metwork Infrusion Detection Systems (MIDS) Image and the Management (SIEM) Image and the Management (SIEM) Metwork Infrusion Detection Systems (MIDS) Image and the Management (SIEM) Image and the Management (SIEM) Data Recovery Image and the Management (SIEM) Image and the Management (SIEM) Network Systems Parket Management (SIEM) Image and the Management (SIEM) Virtual Private Recover (MPN) Image and the Management (SIEM) Virtual Private Recover (MPN) Image and the Management (SIEM)	Firewalls - Virtualized					
Deep Packet Impactson UPPI ApplianceImpact Impactson and Event Management (SIM)Impact Impactson and Event Management (SIM)Impact Impactson And Event Management (SIM)Veb Provies/Conent FilteringImpact Management (SIM)Impact Management (SIM)Impact Impactson Detection (IMEOS)Impact Management (SIM)Impact Management (SIM)Network Intrusion Detection (IMEOS)Impact Management (SIM)Impact Management (SIM)Network Intrusion Prevention Systems (NIDS)Impact Management (SIM)Impact Management (SIM)Network Intrusion Prevention SystemsImpact Management (SIM)Impact Management (SIM)Network Systems Network (SIM)Impact Management (SIM)Impact Manage	Web Application Firewalls					
Security information and Event Management [SIM]Imagement [SIM]Imagement [SIM]Web Prodes/Convert FilteringImagement [SIM]Imagement [SIM]Intrusion Detection /Iverention Systems (INDS)Imagement [SIM]Imagement [SIM]Network Intrusion Detection systems (INDS)Imagement [SIM]Imagement [SIM]Network Intrusion Detection systems (INDS)Imagement [SIM]Imagement [SIM]Network Intrusion Prevention Systems (INDS)Imagement [SIM]Imagement [SIM]Unified Intrast Management (UTM) SystemsImagement [SIM]Imagement [SIM]Unified Intrast Management (UTM) SystemsImagement [SIM]Imagement [SIM]Data Isos Prevention (DUP)Imagement [SIM]Imagement [SIM]Data RecoveryImagement [SIM]Imagement [SIM]Vitrus Private Reverk (VPD)Imagement [SIM]Imagement [SIM]Vitrus Private Reverk (Reverk (SIM]Imagement [SIM]Image	End Point Detection & Response (EDR)					
Web Pooles/Conent Filering Image: Pooles/Conent Filering C Intrusion Detection (HOS) Host Intrusion Detection (HOS) Image: Pooles/Conent Filering Network Intrusion Detection (HOS) Image: Pooles/Conent Filering Network Intrusion Detection (HOS) Image: Pooles/Conent Filering Network Intrusion Detection Systems (HOS) Image: Pooles/Conent Filering Network Intrusion Prevention Systems (HOS) Image: Pooles/Conent Filering Network Intrusion Prevention Systems (HOS) Image: Pooles/Conent Filering Network Tar PI solutions Image: Pooles/Conent Filering Data Loss Prevention (DIP) Image: Pooles/Conent Filering Data Loss Prevention (NPP) Image: Pooles/Conent Filering Network Systems Image: Pooles/Conent Filering Vartualization Software - Barce Metal Hypervisor Image: Pooles/Conent Filering Vartualization Software - Work Station-Bascel Hypervisor Image: Pooles/Conent Filering Vartualization Software - Work Station-Bascel Hypervisor Image: Pooles/Conent Filering Vartualization Software - Work Station-Bascel Hypervisor Image: Pooles/Conent Filering Vartualization Software - Work Station-Bascel Hypervisor Image: Pooles/Conent Filering Software Detection (Hypervisor) Image: Pooles/Conent Filering Software Detection Systems Image: Pooles/Conent Filering <	Deep Packet Inspection (DPI) Appliance					
Intrusion Detection/Prevention SystemsIntrusion Detection (HDS)Intrusion Detection Systems (HDS)Host Intrusion Detection Systems (HDS)Intrusion Prevention Systems (HDS)Intrusion Prevention Systems (HDS)Network Intrusion Prevention Systems (HDS)Intrusion Prevention Systems (HDS)Intrusion Prevention Systems (HDS)Unified Threat Management (UTM) SystemsIntrusion Prevention Systems (HDS)Intrusion Prevention Systems (HDS)Network Intrusion Prevention Systems (HDS)Intrusion Prevention Systems (HDS)Intrusion Prevention Systems (HDS)Data BecoweryIntrusion Prevention SystemsIntrusion Prevention SystemsIntrusion Prevention SystemsData BecoweryIntrusion Software- Intrusion Prevention SystemsIntrusion Prevention SystemsVirtual Private Network (VPN)Intrusion Software- Intrusion Prevention SystemsIntrusion Software- Intrusion Prevention SystemsVirtual Private Network (SDN) SolutionsIntrusion Software- Intrusion Prevention SystemsIntrusion Software- Intrusion Prevention SystemsSoftware Defined Networking (SDN) SolutionsIntrusion Software- Intrusion Prevention SystemsIntrusion Software- Intrusion Prevention SystemsComputer Operating SystemsIntrusion Software- Intrusion Software- Intrusion Software- Intrusion Software- Intrusion Prevention Software- Intrusion Software- I	Security Information and Event Management (SIEM)					
Instruction Detection (HDS) Image: Construction Systems (HDS) Network Intrusion Prevention Systems (HDS) Image: Construction Systems (HDS) Network Intrusion Prevention Systems (HDS) Image: Construction Systems (HDS) Network Intrusion Prevention Systems (HDS) Image: Construction Systems (HDS) Unified Thread Management (UTM) Systems Image: Construction Systems (HDS) Network Tar Pits olutions Image: Construction Systems (HDS) Network Tar Pits olutions Image: Construction Systems Data Loss Prevention (D/P) Image: Construction Systems Network Systems Image: Construction Systems Network Systems Image: Construction Systems Vitrual Private Network (VPN) Image: Construction Systems Software Defined Networking (Stoth) Solutions Image: Construction Systems Image: Construction Systems Image: Construction Systems Image: Construction Systems Image: Construction Systems Networked Printers Image: Construction Systems Netw	Web Proxies/Conent Filtering					
Network intrusion Petention Systems (NIPS)Image: Constraint of Constraint o	C. Intrusion Detection/Prevention Systems					
Host Intrusion Prevention Systems (HIPS)Image: Constraint of Systems (MIPS)Image: Constraint of Systems (MIPS)Network Intrusion Prevention Systems (MIPS)Image: Constraint of Systems (MIPS)Image: Constraint of Systems (MIPS)HoneypotImage: Constraint of Systems (MIPS)Image: Constraint of Systems (MIPS)Network Tar Pit SolutionsImage: Constraint of Systems (MIPS)Image: Constraint of Systems (MIPS)Network SystemsImage: Constraint of Systems (MIPS)Image: Constraint of Systems (MIPS)Network SystemsImage: Constraint of Systems (MIPS)Image: Constraint of Systems (MIPS)Virtual Private Network (VPS)Image: Constraint of Systems (MIPS)Image: Constraint of Systems (MIPS)Virtualization Software - Nork Station-Based HypervisorImage: Constraint of Systems (MIPS)Virtualization Software - Nork Station-Based HypervisorImage: Constraint of Systems (MIPS)Other (Define in Comment Box)Image: Constraint of Systems (MIPS)Software Define Networking (SON) solutionsImage: Constraint of Systems (MIPS)Noble Order Systems - NetworkedImage: Constraint of Systems (MIPS)Software Define Networking SystemsImage: Constraint of Systems (MIPS)Noble Order Operating SystemsImage: Constraint of Systems (MIPS)Noble Order Operating Systems - Network ConnectedImage: Constraint of Systems (MIPS)Networked Printers ConstratedImage: Constraint of Systems (MIPS)Networked Statems - Network ConnectedImage: Constraint of Systems (MIPS)Networked Statems - Network ConnectedImage: Constraint of Systems (MIPS)Phys	Host Intrusion Detection (HIDS)					
Network Intrusion Prevention Systems (NIPS) Image: Comparing Systems (NIPS) Unified Threat Management (UTM) Systems Image: Comparing Systems Honeypot Image: Comparing Systems Data Recovery Image: Comparing Systems Data Recovery Image: Comparing Systems Virtual Private Network (VPN) Image: Comparing Systems Virtual Private Network (VPN) Image: Comparing Systems Virtual Private Sever (VPS) Image: Comparing Systems Other Products Image: Comparing Systems	Network Intrusion Detection Systems (NIDS)					
Unified Threat Management (UTM) Systems Image in the image in t	Host Intrusion Prevention Systems (HIPS)					
HoneypotInclusionInclusionNetwork Tar Pit solutionsImage: Constraint of the solutionsImage: Constraint of the solutionsData Loss Prevention (DLP)Image: Constraint of the solutionsImage: Constraint of the solutionsData RecoveryImage: Constraint of the solutionsImage: Constraint of the solutionsData RecoveryImage: Constraint of the solutionsImage: Constraint of the solutionsData RecoveryImage: Constraint of the solutionsImage: Constraint of the solutionsVirtual Private Network (VPN)Image: Constraint of the solutionsImage: Constraint of the solutionsVirtualization Software - Bare Metal HypervisorImage: Constraint of the solutionsImage: Constraint of the solutionsVirtualization Software - Bare Metal HypervisorImage: Constraint of the solutionsImage: Constraint of the solutionsSoftware Defined Networking (SDN) solutionsImage: Constraint of the solutionsImage: Constraint of the solutionsOther ProductsImage: Constraint of the solution (SCADA)-NetworkedImage: Constraint of the solution (SCADA)-NetworkedComputer Constraint of Data Acquisition (SCADA)-NetworkedImage: Constraint of the solution (SCADA)-NetworkedComputer SolutionsImage: Constraint of the solution (SCADA)-NetworkedImage: Constraint of the solution (SCADA)-NetworkedMulti-Function Devices Printers Constraint of the solution (SCADA)-NetworkedImage: Constraint of the solution (SCADA)-NetworkedNetworked PrintersImage: Constraint of the solution (SCADA)-NetworkedImage: Constraint of the solution (SCADA)-NetworkedNetworked Printers	Network Intrusion Prevention Systems (NIPS)					
Network Tar Pit solutions Image: Constraint of D(P) Data Loss Prevention (D(P) Image: Constraint of Con	Unified Threat Management (UTM) Systems					
Data Loss Prevention (DLP) Image: Constraint of the cons	Honeypot					
Data RecoveryData RecoveryImage: Constraint of the	Network Tar Pit solutions					
Network SystemsImage: Systems	Data Loss Prevention (DLP)					
Virtual Private Network (VPN)Image: Constraint of Constraint						
Virtual Private Server (VPS)Image: Constraint of the server (VPS)Image: Constraint of the server (VPS)Virtualization Software - Bare Metal HypervisorImage: Constraint of the server (VPS)Image: Constraint of the server (VPS)Virtualization Software - Work Station-Based HypervisorImage: Constraint of the server (VPS)Image: Constraint of the server (VPS)Software Defined Networking (SDN) solutionsImage: Constraint of the server (VPS)Image: Constraint of the server (VPS)Software Defined Networking (SDN) solutionsImage: Constraint of the server (VPS)Image: Constraint of the server (VPS)Other [Define in comment Box]Image: Constraint of the server (VPS)Image: Constraint of the server (VPS)Industrial Control Systems - NetworkedImage: Constraint of the server (VPS)Image: Constraint of the server (VPS)Systems-On-Chip, Microcontroller DevicesImage: Constraint of the server (VPS)Image: Constraint of the server (VPS)Multi-Function Devices - Printers-Copiers-ScannersImage: Constraint of the server (Constraint of the server (Constra	D. Network Systems					
Virtualization Software - Bare Metal Hypervisor Image: Comparison of	Virtual Private Network (VPN)					
Virtualization Software - Work Station-Based HypervisorImage: Constraint of	Virtual Private Server (VPS)					
Software Defined Networking (SDN) solutionsImage: Software Defined Networking (SDN) solutionsImage: Software Defined Networking (SDN) solutionsOther [Define in Comment Box]Image: Software Defined NetworkedImage: Software Defined NetworkedIndustrial Control Systems - NetworkedImage: Software Defined NetworkedImage: Software Defined NetworkedIndustrial Control Systems - NetworkedImage: Software Defined NetworkedImage: Software Defined NetworkedSupervisory Control and Data Acquisition (SCADA)-NetworkedImage: Software Defined Networked NetworkedImage: Software Defined Networked NetworkedComputer Operating SystemsImage: Software Defined Networked PrintersImage: Software Defined Networked PrintersMulti-Function Devices - Printers-Copiers-ScannersImage: Software Defined Networked PrintersImage: Software Defined Networked PrintersNetworked PrintersImage: Software Network ConnectedImage: Software Defined Networked PrintersImage: Software Defined Networked PrintersHealth Management Systems - Network ConnectedImage: Software Defined Networked PrintersImage: Software Defined Networked PrintersPhysical Access Control Systems - Network ConnectedImage: Software Defined Networked PrintersImage: Software Defined Networked PrintersPhysical Security Video Monitoring Systems - Network ConnectedImage: Software Defined Networked PrintersImage: Software Defined Networked PrintersPhysical Security Video Monitoring Systems - Network ConnectedImage: Software Defined Networked PrintersImage: Software Defined Networked						
Other [Define in Comment Box]Image: Comment Box]Image: Comment Box]Other ProductsImage: Comment Box]Image: Comment Box]Industrial Control Systems - NetworkedImage: Comment Box]Image: Comment Box]Supervisory Control and Data Acquisition (SCADA)-NetworkedImage: Comment Box]Image: Comment Box]Computer Operating SystemsImage: Comment Box]Image: Comment Box]Computer FirmwareImage: Comment Box]Image: Comment Box]Systems-On-Chip, Microcontroller DevicesImage: Comment Box]Image: Comment Box]Multi-Function Devices - Printers-Copiers-ScannersImage: Comment Box]Image: Comment Box]Multi-Function Devices - Printers-Copiers-ScannersImage: Comment Box]Image: Comment Box]Networked ScannersImage: Comment Box]Image: Comment Box]Image: Comment Box]Health Management Systems - Network ConnectedImage: Comment Box]Image: Comment Box]Physical Security Video Monitoring Systems - Network ConnectedImage: Comment Box]Image: Comment Box]Physical Security Video Monitoring Systems - Network ConnectedImage: Comment Box]Image: Comment Box]Comments:Image: Comment Box]Image: Comment Box]Image: Commen						
Dther Products Image: Control Systems - Networked Supervisory Control and Data Acquisition (SCADA)-Networked Image: Computer Operating Systems Computer Operating Systems Image: Computer Firmware Computer Firmware Image: Computer Operating Systems Systems-On-Chip, Microcontroller Devices Image: Computer Systems Mobile Device Operating Systems Image: Computer Systems Multi-Function Devices - Printers-Copiers-Scanners Image: Computer Systems Networked Frinters Image: Computer Systems - Network Connected Health Management Systems - Network Connected Image: Computer Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected Image: Computer Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected Image: Computer Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected Image: Computer Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected Image: Computer Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected Image: Computer Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected Image: Computer Systems - Network Connected Comments: Image: Computer S						
Industrial Control Systems - NetworkedImage with Systems - Network ConnectedImage with Systems - Network ConnectedHealth Systems / Network ConnectedImage with Systems - Network ConnectedImage with Systems - Network ConnectedPhysical Security Video Monitoring Systems - Network ConnectedImage with Systems - Network ConnectedImage with Systems - Network ConnectedPhysical Security Video Monitoring Systems - Network ConnectedImage with Systems - Network ConnectedImage with Systems - Network ConnectedPhysical Security Video Monitoring Systems - Network ConnectedImage with Systems - Network ConnectedImage with Systems - Network ConnectedComments:Image with Systems - Network ConnectedImage with Systems - Network ConnectedImage with Systems - Network ConnectedPhysical Security Video Monitoring Systems - Network ConnectedImage with Systems - Network ConnectedImage with Systems - Network ConnectedPhysical Security Video Monitoring Systems - Network ConnectedImage with Systems - Network ConnectedImage with Systems - Network ConnectedPhysical Security Video Monitoring Systems - Network ConnectedImage with Systems - Network ConnectedImage with Systems - Network ConnectedPhysical Security Video Monitoring Systems - Network ConnectedImage with Systems - Network ConnectedImage with Systems - Network ConnectedPhysical Security Video Monitoring Systems - Network ConnectedImage with Systems - Network ConnectedImage with Systems - Network ConnectedPhysical Security Video Monitoring Systems - Network ConnectedImage with Systems - Network ConnectedImage with Systems - Network Connected						
Supervisory Control and Data Acquisition (SCADA)-NetworkedImage: Computer Operating SystemsComputer Operating SystemsImage: Computer FirmwareComputer FirmwareImage: Computer FirmwareSystems-On-Chip, Microcontroller DevicesImage: Computer SystemsMobile Device Operating SystemsImage: Computer SystemsMobile Devices Operating SystemsImage: Computer SystemsMulti-Function Devices - Printers-Copiers-ScannersImage: Computer SystemsNetworked PrintersImage: Computer Systems - Network ConnectedHealth Management Systems - Network ConnectedImage: Computer Systems - Network ConnectedPhysical Access Control Systems - Network ConnectedImage: Computer Systems - Network ConnectedPhysical Access Systems (Audio & Video Conferencing Systems)Image: Comments:Comments:Image: Comments:Comments:Image: Computer SystemsComments:Image: Comments:						
Computer Operating SystemsComputer Operating SystemsComputer S						
Computer FirmwareImage: Computer Size Size Size Size Size Size Size Size						
Systems-On-Chip, Microcontroller Devices Image: Control Systems Mobile Device Operating Systems Image: Control Systems Multi-Function Devices - Printers-Copiers-Scanners Image: Control Systems Multi-Function Devices - Printers-Copiers-Scanners Image: Control Systems Networked Frinters Image: Control Systems Networked Scanners Image: Control Systems - Network Connected Health Management Systems - Network Connected Image: Control Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected Image: Control Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected Image: Control Systems - Network Connected Comments: Image: Control Systems - Network Connected Image: Control Systems - Network Connected						
Mobile Device Operating Systems Mobile Device Operating Systems Multi-Function Devices - Printers-Copiers-Scanners Mobile Device Operating Systems Networked Printers Mobile Device Operating Systems Networked Scanners Mobile Device Operating Systems - Network Connected Health Management Systems - Network Connected Mobile Device Operating Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected Mobile Device Operating Systems - Network Connected Physical Security Video Monitoring Systems - Network Connected Mobile Device Operating Systems - Network Connected Telepresence Systems (Audio & Video Conferencing Systems) Mobile Device Operating Systems - Network Connected Comments: Mobile Device Systems Mobile Device Systems						
Multi-Function Devices - Printers-Copiers-Scanners Image: Comparise of the state of the s						
Networked Printers Image: Comparison of the comparison						
Networked Scanners Image: Network Connected Health Management Systems - Network Connected Image: Network Connected Health Systems / Network Connected Image: Network Connected Physical Access Control Systems - Network Connected Image: Network Connected Physical Security Video Monitoring Systems - Network Connected Image: Network Connected Telepresence Systems (Audio & Video Conferencing Systems) Image: Network Connected Comments: Image: Network Conferencing Systems)				-		
Health Management Systems - Network Connected Image: Connected Health Systems/Devices - Network Connected Image: Connected Physical Security Video Monitoring Systems - Network Connected Image: Connected Physical Security Video Monitoring Systems - Network Connected Image: Connected Telepresence Systems (Audio & Video Conferencing Systems) Image: Conments: Comments: Image: Content Systems - Content Systems						
Health Systems/Devices - Network Connected Image: Connected Connected Physical Access Control Systems - Network Connected Image: Connected Connected Physical Security Video Monitoring Systems - Network Connected Image: Connected Connected Telepresence Systems (Audio & Video Conferencing Systems) Image: Conments: Comments: Image: Connected Con						
Physical Access Control Systems - Network Connected Image: Connected Connected Physical Security Video Monitoring Systems - Network Connected Image: Connected Connected Connected Telepresence Systems (Audio & Video Conferencing Systems) Image: Conments: Comments: Image: Connected Co						
Physical Security Video Monitoring Systems - Network Connected Image: Connected Connected Telepresence Systems (Audio & Video Conferencing Systems) Image: Connected						
Telepresence Systems (Audio & Video Conferencing Systems) Image: Comments: Comments:		_				
Comments:						
BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act			<u> </u>			

Previous Page																				Next Page
tion 3.a - Integration/Embedding of X/Z technologies into Manufacturers Information Technology Products - Telemetry I: Direct Comm, Types of Comm																				
ution-																				
uction: entify the products made or marketed by your company that incorporate XYZ software or associated XYZ services that allow your organization's products to communicate with XYZ security network, XYZ infrastructure, and XYZ affiliates.																				
pecify the types of communications that your organization's products send or receive through XYZ networks.																				
ate the typics of communications alerty/events that are associated with the products marketed by your organization that incorporte XYZ software.																				
an advantional product indices namines as introduced in advancement product indices indices and produce realized on screening this page to the right s = = =																				
Communicates with XYZ Connected Systems Types of Communications Received/Sent Detection Development/Jet Tevens																				
																				i i
	#1 Your Company's Product	XYZ Security	XYZ		Other (Use	No XYZ		Bug Fix	System	Remote	System	System		Detection	Detection Events,	Detection events,	Cloud scanning,	Cloud Scanning,	Other Alert,	Other Aler
Types of Devices that Communicate With XYZ	Series/Model	Network	Infrastructure	XYZ Affiliate	Comment	Telemetry	Alerts	Reports	Operations	Command /Control	Performance Data	Updates	User Data	Events, No Data	Sample	Sample	Sample	Sample	No User Data	User Data
	Number				Box)					/ Control	Data			NO Data	Hashes	Content	Sashes	Content	Data	
																				i i
A. Network Infrastructure Devices	Auto Populate																			
Routers		Hardware																		
Switches Gateways - Internet		Software Both																	\vdash	ļ
Gateways - Internet Gateways - Internet Service Provider Grade		None		-										-					<u> </u>	-
Gateways - Cloud								1												
Gateway - Modular Internet-of-Things (IoT)																				
Mobile Secure Gateways																				
B. Network Security Devices																				
Antivirus Scanning Application - Host Based Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)						+		-											\vdash	
Firewalls - Host Based																				
Firewalls - Network Appliance																				
Firewalls - Cloud																				
Firewalls - Virtualized Web Application Firewalls																				
End Point Detection & Response (EDR)																			$ \rightarrow $	
Deep Packet Inspection (DPI) Appliance																				
Security Information and Event Management (SIEM)																				
Web Proxies/Conent Filtering																				-
C. Intrusion Detection/Prevention Systems Host Intrusion Detection (HIDS)																				
Host Intrusion Detection (HIDS) Network Intrusion Detection Systems (NIDS)																			L	
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																				-
D. Network Systems																				
Virtual Private Network (VPN)																				
Virtual Private Server (VPS) Virtualization Software - Bare Metal Hypervisor																				<u> </u>
Virtualization Software - Bare Metal Hypervisor Virtualization Software - Work Station-Based Hypervisor				-															\vdash	-
Software Defined Networking (SDN) solutions						1														
Other [Define in Comment Box]																				
E. Other Products	-																			
Industrial Control Systems - Networked Supervisory Control and Data Acquisition (SCADA)-Networked				-		-		I			-								\vdash	
Computer Operating Systems				-		-		1												
Computer Firmware								1												
Systems-On-Chip, Microcontroller Devices																				
Mobile Device Operating Systems Multi-Function Devices - Printers-Copiers-Scanners																				—
Multi-Function Devices - Printers-Copiers-scanners Networked Printers		-		-													-		<u>├</u>	-
Networked Scanners				-		1		1												
Health Management Systems - Network Connected				1		+		1											<u> </u>	
Health Systems/Devices - Network Connected								1												
Physical Access Control Systems - Network Connected																				
Physical Security Video Monitoring Systems - Network Connected	-																			
Telepresence Systems (Audio & Video Conferencing Systems) Comments:		-						I											\vdash	
Commence.		L		RUSINESS	CONFIDENT	IAI - Der Se	tion 705(d)	I of the Defe	nse Producti	on Act	L	I						L		·
				POSINESS	CONTIDENT	Inter Per Sei		or the pere	nac FroudCti	ALL NO.										

Previous Page Section 3.b - Integration/Embedding of XYZ technologies into Manufacturers Information Technology Products - Telemetry 2: Receiving Methods, Returning Info

Next Page

Instruction: For the products reported in Section 3.a as utilizing XYZ software or associated XYZ services that allow your organization's products to communicate with the XYZ Security Network; Other XYZ Company infrastructure; or Third-Parties with known supporting-contract relationships with XYZ company, identify the: 1) Methods used for Receiving Updates, Signatures, Instructions 2) Modes used for Returning Information Directly Back to XYZ Company

Enter all additional product model numbers. Information on additional product model numbers may be entered in form blocks reached by scrolling this page to the right 000

Interclust Status Sta		Integration	Integration of XYZ Software, Hardware, & Services in Information Technology Systems - Methods for Receiving/Modes for Returning Information											
Preductional communicationDescriptional constructional c		Methods for Rec	eiving Upda	tes, Signatu	res, Instructi	ons	Modes for Directly E	Returning Ir Back to XYZ (nformation Company					
backerback	Types of Devices that Communicate	Company's Product Series/Model		Self-Hosted Mirror	Firmware Update	Other (Use Comment Box)	Direct Connection to XYZ	Self-Hosted Aggregator	Other (Use Comment Box)	Comments				
wheneServerServe	Network Infrastructure Devices	Auto-Populate												
IntervalImageImageImageImageImageImageImageCataryay-HourdImageImageImageImageImageImageImageCataryay-HourdImageImageImageImageImageImageImageImageAbdiaCataryay-HourdImage <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>														
Interval Columa 														
Internet-Shing)Internet-Shing)Internet-Shing)Internet-Shing)Internet-Shing)Idexw-Moke Internet-Shing)Idex IIdex														
checkerschecke			None											
Note: <th< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>														
Network Scaruly DevicesNetwork Scaruly Scaru														
Intrivis canning appliancesInterfactor statesInterfactor states <td></td>														
Not/Againation ControlImage Control<														
IncludeImage: Sector Sect	Antivirus scanning appliances													
iFreedia-ViralizedImage: CloudImage:	Firewalls - Host/Application Side													
iFreedingImage: VirtualisedImage: Virtua	Firewalls - Network Side													
Web Application FierwallsImage and the subsection (SPI)Image														
ind Point Detection & Response (DB)Image and the sector of Point Management (SIEM)Image and the sector of P														
Deep Pocket Inguschin (PP)Imagement (SIEM)Imagement (SIEM) <td></td>														
Security Information and Event Management (DRM)Image and the section Approach FilteringImage and the section Approach FilteringImage and the section Approach (DRA)Intrusion Detection/Prevention SystemsImage and the section Approach (DRA)Image and the section Approach (DRA)Image and the section Approach (DRA)Intrusion Detection/Prevention Systems (NDD).Image and the section Approach (DRA)Image and the section Approach (DRA)Image and the section Approach (DRA)Network Intrusion Detection Systems (NDD).Image and the section Approach (DRA)Image and the section Approach (DRA)Image and the section Approach (DRA)Network Intrusion Detection Systems (NDD).Image and the section Approach (DRA)Image and the section Approach (DRA)Image and the section Approach (DRA)Network Intrusion Detection Systems (NDD).Image and the section Approach (DRA)Image and the section Approach (DRA)Image and the section Approach (DRA)Network Tar Pit solutionsImage and the section (DRA)Image and the section (DRA)Image and the section Approach (DRA)Data Loss Prevention Systems (NDD)Image and the section (DRA)Image and the section (DRA)Image and the section (DRA)Virtual Private Systems (NDN)Image and the section (DRA)Image and the section (DRA)Image and the section (DRA)Other Detection Approach (DRA)Image and the section (DRA)Image and the section (DRA)Virtual Private Section Approach (DRA)Image and the section (DRA)Image and the section (DRA)Other Define In Comment Bon)Image and the section (DRA)Image and the section (DRA)Dispere														
Web Product/Concert FilteringImage of the state of the sta														
Intrusion Detection/Prevention Systems (INDS)Image and the s														
Intrusion Detection (NDS)- Host Intrusion Detection (NDS)- Network Intrusion (NDS)- Network Intrusion Detection (NDS)- Network Intrusion Detection (NDS)- Network Intrusion (NDS)														
i-host intrusion Detection (HDS)IIIIIIntrusion Detection Systems (IDS)- Network intrusion Detection Systems (IMPS)IIIINetwork intrusion Prevention Systems (IMPS)IIIIIUnified Threat Management (UTM) SystemsIIIIIUnified Threat Management (UTM) Systems (IMPS)IIIIIUnified Threat Management (UTM) SystemsIIIIIIData Loss Prevention Systems (IMPS)IIIIIINetwork Tar Pit solutionsIIIIIIData Loss Prevention Systems (IMPS)IIIIIINetwork SystemsIIIIIIIVirtual Private Network (VPN)IIIIIIIVirtual Private Network (VPN)IIIIIIIVirtual Private Network (ISD) solutionsIIIIIIIOther (Define In Comment Bod)IIIIIIIIIndustrial Control Systems - NetworkdIIIIIIIISupervisor Control and Data Acquisition (SCADA)IIIIIIIIIndustrial Control Systems - NetworkdIIIIIIIII<														
Hott Intrusion Prevention Systems (HIPS) Image (Construction Prevention Systems (NPS)) Image (Construction Prevention Prevention Systems (NPS)) Image (Construction Prevention Prevented Prevention Prevention Prevention Prevention Pre	Host Intrusion Detection (HIDS) Intrusion Detection Systems (IDS) -													
Network Intrusion Revention Systems (NPS)Image and the systems of the s														
Unifed Threat Management (UTM) SystemsImagement (UTM) Systems <th< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>														
HoneypotIndex<														
Network Tar Pit solutionsNetwork Tar Pit solution														
Data loss Prevention (DLP)Image: Constraint of the constrai														
Data RecoveryData RecoveryImage: Constraint of the														
Network SystemsImage: Systems Systems SystemsImage: Systems Systems Systems SystemsImage: Systems S														
Virtual Private Server (VPS) Image: Constraint of Constr														
Virtualization SoftwareImage: Software Defined Networking (SDN) solutionsImage: Software Defined Networking Networking (SDN) solutionsImage: Software Defined Networking Netwo														
Software Defined Networking (SDN) solutionsImage: Software Defined Networking Netwo	Virtual Private Server (VPS)													
Other (Define in Comment Box) Image: Set Worked														
Other ProductsOther ProductsImage: Control Systems - NetworkedImage:														
Industrial Control Systems - NetworkedImage: Supervisory Control and Data Acquisition (SCADA)Image: Supervisory Control and Data Acquisition (SCADA)Image: Supervisory Control and Data Acquisition (SCADA)Supervisory Control and Data Acquisition (SCADA)Image: Supervisory Control and Data Acquisition (SCADA)Image: Supervisory Control and Data Acquisition (SCADA)Computer Operating SystemsImage: Supervisory Control and Data Acquisition (SCADA)Image: Supervisory Control and Data Acquisition (SCADA)Integrated Circuit ProductsImage: Supervisory Control and Data Acquisition (SCADA)Image: Supervisory Control and Data Acquisition (SCADA)Integrated Circuit ProductsImage: Supervisory Control and Data Acquisition (SCADA)Image: Supervisory Control and Systems (Audio & Video Conferencin														
Spervisory Control and Data Acquisition (SCADA) Image: Specific S														
Computer Operating Systems Integrated Circuit Products Integrated Circuit Products Integrated Circuit Products Integrated Circuit Products Image: Computer Operating Systems Image: Computer Operating Systems Image: Computer Operating Systems Image: Computer Operating Systems Mobile Device Operating Systems Image: Computer Operating Systems I	Supervisory Control and Data Acquisition (SCADA)													
Integrated Circuit Products (processors, memory, microcontrollers) Image: Systems Image: System														
Multi-Function Devices - Printers-Copiers-Scanners Image: Copiers - Scanners Image: Copiers - Scann	Integrated Circuit Products (processors, memory, microcontrollers)													
Health Systems/Devices - Network Connected Image: Connected Image														
Physical Access Control Systems - Electron. Network Connected Image: Control Systems - Electron. Physical Security Video Monitoring Systems - Network Connected Image: Control Systems - Electron. Telepresence Systems (Audio & Video Conferencing Systems) Image: Control Systems - Electron.														
Physical Security Video Monitoring Systems - Network Connected Telepresence Systems (Audio & Video Conferencing Systems)	Physical Access Control Systems - Electron.													
Telepresence Systems (Audio & Video Conferencing Systems)	Physical Security Video Monitoring Systems													
	Telepresence Systems (Audio & Video Conferencing													

Section 3.c - Integration/Embedding of XYZ technologies into Manufacturers Information Technology Products - Telemetry 3: Passive Indicators, All Indicators

Next Page

Instruction: For the information technology products reported in Section 3.a as utilizing. XYZ software or associated XYZ services that allow your organization's products to communicate with the XYZ Security Network; Other XYZ Company infrastructure; or Third-Parties with known supporting-contract relationships with XYZ company, identify the:

Indicators for Passively Detecting XYZ in Information Technology Products
 Report All Indicators Associated With Communications With XYZ Organizations

Integration of XYZ Software, Hardware, & Services in Hardware Systems - Passive Detection in Hardware/Communications Indicators Indicators for Passively Detecting XYZ in Information Technology Report All Indicators Associated With Products Communications With XYZ Organizations Other (Use omment Box) Internet Protoc Addresses Other (Use omment Do> nstructions #1 Your Signature Indica Updates Domains Company's Product Types of Devices that Communicate Directly Comments Series/Model iaue Number Network Infrastructure Devices Auto-Populate Routers Hardware Software Switches Gateways - Internet Both Gateways - Internet-to-Orbit None Gateways - Cloud Gateway - Modular Internet-of-Things (IoT) Mobile Secure Gateways Network Security Devices Antivirus scanning appliances - Host-based Antivirus scanning appliances - Gateway-based scanning Firewalls - Host/Application Side Firewalls - Network Side Firewalls - Cloud Firewalls - Virtualized Web Application Firewalls End Point Detection & Response (EDR) Deep Packet Inspection (DPI) Security Information and Event Management (SIEM) Web Proxies/Conent Filtering Intrusion Detection/Prevention Systems Intrusion Detection Systems (IDS) - Host Intrusion Detection (HIDS) Intrusion Detection Systems (IDS) -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 Network Systems Virtual Private Network (VPN) Virtual Private Server (VPS) Virtualization Software Software Defined Networking (SDN) solutions Other (Define in Comment Box) Other Products Industrial Control Systems - Networked Supervisory Control and Data Acquisition (SCADA) -Networked Computer Operating Systems Integrated Circuit Products (processors, memory, microcontrollers) Mobile Device Operating Systems Multi-Function Devices - Printers-Copiers-Scanners Health Systems/Devices - Network Connected Physical Access Control Systems - Electron. Network Connected Physical Security Video Monitoring Systems - Network Connected Telepresence Systems (Audio & Video Conferencing Systems) Comments: BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

lentify the practices that your company, since 2014, has actively performed with regard to any products it sells that incorporate third-party technologies. Hardware/Software Products Sold Maintains a Current Maintains a Current Maintains a Current Maintains a Current List of the Names of Executable Maintains a List of Suppliers of Executable Maintains a List of Supplices of Executable <th><u>revious Page</u> ection 4 - Practices for Tracking Technologies Used I</th> <th>n Hardware & Sof</th> <th>ftware Network</th> <th>Products Sold By Your (</th> <th>Organization</th> <th></th> <th></th> <th></th> <th><u>Next Page</u></th>	<u>revious Page</u> ection 4 - Practices for Tracking Technologies Used I	n Hardware & Sof	ftware Network	Products Sold By Your (Organization				<u>Next Page</u>
Markarcodowney backs of law thrower with and an additional set of provided and additional set of provided and additional set of provided additional set of provide									
balancepole <t< th=""><th>By Your Organization</th><th>List of Third-Party Components Used in</th><th>List of Third-Party Components Used in</th><th>Names of Executable Components in its Hardware</th><th>Suppliers of Executable Components Used by</th><th>Known Vulnerabilities Associated With Third- Party Executable</th><th>Known Vulnerabilities Associated With Organization-Owned</th><th>company products that contain XYZ</th><th>Commen</th></t<>	By Your Organization	List of Third-Party Components Used in	List of Third-Party Components Used in	Names of Executable Components in its Hardware	Suppliers of Executable Components Used by	Known Vulnerabilities Associated With Third- Party Executable	Known Vulnerabilities Associated With Organization-Owned	company products that contain XYZ	Commen
bordSoldS	Network Infrastructure Devices	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	
wheedwheedIII									
sintersint									
above <th< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>									
chelmschelm <th< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>									
Advach ResultMakabia frame Advach ResultMather Advach ResultMather Advach ResultMather Advach ResultMather Advach ResultMather Advach ResultMather Advach ResultMather ResultMather ResultMather ResultMather ResultMather ResultMather ResultMather ResultMather ResultMather ResultMather ResultMather ResultMather ResultMather 									
Noise <th< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>									
Network<									
ArbityArbit									
InterfaceIndex <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>									
Investion <td></td> <td>-</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>		-							
inval.inval									
invalsinval									
investinginterfact									
whe Application FreevalsImage: Application Servery (APS)Image: Application Servery (A									
Indicates is 6 Regioner (DM)Image									
beskimagei									
sextry indication and new Management (BM)Indication SectorIndication SectorInd	• • • •								
Web Provide View of Private Pr									
Intradio Detection /RDSImage									
Instantion Detection Systems (NIPS)Image: Similar Systems (NIPS)Image: Sim									
lethow hitmaion Detection Systems (NDS)Image and (NDS									
isotis	Host Intrusion Detection (HIDS)								
betwork htmision Prevention Systems (https:)Image met (UTM) SystemsImage met (UTM) Systems </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>									
Industrial format wangement (UTM) systemsInc.	Host Intrusion Prevention Systems (HIPS)								
Honopot Network Tar Pit solutionsIncome of the solution of the solutionsIncome of the so	Network Intrusion Prevention Systems (NIPS)								
Network Tar Pit solutionsImage: solution (DP)Image: solution (DP) <td>Unified Threat Management (UTM) Systems</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Unified Threat Management (UTM) Systems								
Data less Prevention (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Data less Prevention (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Data less Prevention (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Network SystemsImage: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Virtual Private Network (VPN)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Virtual Private Network (SORN)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Virtual Private Network (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Virtualization Software - Bind Network (SORN)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Other ProductImage: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Systems On Chip, Microcontroller DevicesImage: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Networked StructesImage: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Image: Construction (DLP)Networked StructesImage: Const	Honeypot								
Data RecoveryIndex<	Network Tar Pit solutions								
Network SystemsImage: systemsImage	Data Loss Prevention (DLP)								
Virtual Private Network (VPN)Image: Note of the serve (VPS)Image: Note of the serve (VPS)Ima	Data Recovery								
Virtual Private Server (VPS)Image: Constraint of Constraint o	Network Systems								
Virtualization Software - Bare Metal HypervisorImage: Bare Hyper	Virtual Private Network (VPN)								
Virtualization Software - Work Station-Based HypervisorImage: Software Defined Networking (SDN) solutionsImage: Software Defined Networking (SDN)Image: Software Defi	Virtual Private Server (VPS)								
Software Defined Networking (SDN) solutionsImage: Software Define in Comment Box)Image: Software Define In Comment Box)Imag	Virtualization Software - Bare Metal Hypervisor								
Other [Define in Comment Box]Image: Comparison of Control and Data Acquisition (SCADA)-NetworkedImage: Comparison of Control and Data Acquisition (SCADA)-Networked)Image: Comparis	Virtualization Software - Work Station-Based Hypervisor								
Other ProductsIndextial Control Systems - NetworkedIndextial Control Systems - NetworkedIndextial Control Systems - NetworkedIndextial Control Systems - Network ConnectedIndextial Control Systems - Netwo	Software Defined Networking (SDN) solutions								
Industrial Control Systems - NetworkedImage and the systems of the syst	Other [Define in Comment Box]								
Supervisory Control and Data Acquisition (SCADA)-NetworkedImage: Computer Operating SystemsImage: Computer SystemsI	Other Products								
Computer Operating SystemsComputer FirmwareImage and the systemsImage and the syste	Industrial Control Systems - Networked								
Computer FirmwareImage: Computer SimmwareImage: Computer Simmware	Supervisory Control and Data Acquisition (SCADA)-Networked								
Systems-On-Chip, Microcontroller DevicesSystems-On-Chip, Microcontroller DevicesImage: Control SystemsImage: Con	Computer Operating Systems								
Mobile Device Operating Systems Mobile Device Operating Systems Image: Comparison of the compar	Computer Firmware								
Multi-Function Devices - Printers-Copiers-Scanners Image: Copiers-Scanners Image: Copiers-Scanners <td< td=""><td>Systems-On-Chip, Microcontroller Devices</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	Systems-On-Chip, Microcontroller Devices								
Networked Printers Image: Constraint of the systems of the system	Mobile Device Operating Systems								
Networked Scanners Image: Steps - Network Connected Image: Steps	Multi-Function Devices - Printers-Copiers-Scanners								
Health Management Systems - Network Connected Image: Constraint of the systems - Network - Connected Image: Constraint of the systems - Network - Connected Image: Constraint of the systems - Network - Connected Image: Constraint of the systems - Network - Connected Image: Constraint of the systems - Network - Connected Image: Constraint of the systems - Network - Connected Image: Constraint of the systems - Network - Connected Image: Constraint of the systems - Network - Connected Image: Constraint of the systems -	Networked Printers								
Health Systems/Devices - Network Connected Image: Control Systems - Network - Control Systems - Network	Networked Scanners								
Health Systems/Devices - Network ConnectedImage: Systems - Network ConnectedI									
Physical Access Control Systems - Network Connected Image: Control Systems - Network -									
Physical Security Video Monitoring Systems - Network Connected Image: Control of the system of t	Physical Access Control Systems - Network Connected								
Telepresence Systems (Audio & Video Conferencing Systems)									

Previous F Section	age 5.a Sales and Balance Sheet					<u>Next Pag</u>
From 2014	4-2018 provide your organization's U.S. and non-U.S. sales ir	nformation.				
	Reporting Schedule:		Level of	Report:		
Recor	d \$ in Thousands, e.g. \$12,000.00 = survey input of \$12	2014	2015	2016	2017	2018
Α.	Total Sales, all Customers U.S./Non-U.S. (in \$)					
В.	Total Defense-Related Sales, all Customers U.S./Non-U.S. (in \$)					
C.	Total Information Communication Technology Hardware, Software and Related Sales, all Customers U.S./Non-U.S. (in \$)					
	Income Statement (Select Line Items):		Record \$ in Thousan	ds, e.g. \$12,000.00 = :	survey input of \$12	
	income Statement (Select Line items).	2014	2015	2016	2017	2018
A.	Net Sales (and other revenue)					
В.	Cost of Goods Sold					
C.	Total Operating Income (Loss)					
D.	Earnings Before Interest and Taxes					
E.	Net Income					
	Comments:			·	· · · · · · · · · · · · · · · · · · ·	
	re of financial information is required for both public and on Act (FOIA) requests. Providing BIS with financial info					om Freedom of
	BUSINESS CONFI	DENTIAL - Per Sectio	n 705(d) of the Defense	Production Act		

Previous Pa Section :		earch & Development and Capital Expenditures					<u>Next Pag</u>
Α.	Does you	r organization perform Research and Development (R&D)?		Ye	s/No	lf "No", leave part B bl	ank.
n Part B, r	ecord your	organization's total R&D expenditures for 2014-2018.					
		Reporting Schedule:					
				Record \$ in Thousa	ands, e.g. \$12,000.00	= survey input of \$12	
			2014	2015	2016	2017	2018
	1	Total R&D Expenditures					
В.	2	Total Information Network Hardware, Software and Related Product R&D Expenditures					
	3	Basic Research (as a % of B2)					
	4	Applied Research (as a % of B2)					
	5	Product/Process Development (as a % of B2)					
	Total of 3	3 - 5 (must equal 100%)	0%	0%	0%	0%	0%
n Part C, r	eport your	organization's capital expenditures for 2014-2018. If your organization had no capi	tal expenditures in this	period enter "0" for ea	ach year.		
		Capital Expenditure Reporting Schedule:					
				Record \$ in Thousa	ands, e.g. \$12,000.00	= survey input of \$12	
		Capital Expenditure Category	2014	2015	2016	2017	2018
	1	Total Capital Expenditures					
C.	2	Total Information Communication Technology Hardware, Software and Related Product Capital Expenditures					
	3	Machinery and Equipment (as a % of A2)					
	4	IT, Computers, Software (as a % of A2)					
	5	Land, Buildings, and Leasehold Improvements (as a % of A2)					
	6	Other (as a % of A2)	(specify here)				
	Lines 3 t	hrough 6 must total 100%					
	Com	iments:					
		BUSINESS CONFIDENTIAL - Per Se	ction 705(d) of the De	efense Production A	rt		

Prev	vious Pa	age							<u>Next Page</u>
Sect	ion 6: I	Employ	yment						
			tal number of FTE employees and contractors at this facility for cale and non-U.S. citizens. Do not double count personnel who may per			mate the perc	entage of FTE e	mployees and	contractors
			Reporting Schedule:						
				2014	2015	2016	2017	2018	
А.	1		FTE Employees		ļ			L	
		а	FTE Employees - U.S. Citizens (as a % of line 1)					I	
		b	FTE Employees - non-U.S. Citizens (as a % of line 1)					L	
	2	T	FTE Contractors						
		а	FTE Contractors - U.S. Citizens (as a % of line 2)		1			[1
		b	FTE Contractors - non-U.S. Citizens (as a % of line 2)		1			[1
			ve countries (other than the U.S.) from which your facility has non-l card holder associated with each country.	U.S. citizen workers	s (employees or	r contractors),	, and identify the	e number of e	ach type of
			Country	H-1B	H-2B	F-1	Green Card	0-1	Other
В.	<u> </u>							 	
							-	<u> </u>	
			_						
	Comme	ents:							
			BUSINESS CONFIDENTIAL - Per Sect	tion 705(d) of the [Defense Produc	tion Act			

Prev	ious	Page
1101	1045	1 4 5 6

Select all the issues that your organization faced from 2014 to present then rank the top five issues (1 being most important, 5 being least important). Next, select all the issues that your organization expects to face from 2018-2022 and rank the top five issues. Then explain.

	2014 to	Present	2019-	2023	
Issue	-Yes/No-	Rank	-Yes/No-	Rank	Explain
Aging equipment, facilities, or infrastructure	Yes				
Aging workforce	No				
Competition - domestic					
Competition - foreign					
Counterfeit parts					
Cybersecurity					
Environmental regulations/remediation - U.S.					
Environmental regulations/remediation - non-U.S.					
Export controls (ITAR/USML and/or EAR/CCL)					
Forced localization (e.g. joint venture requirement, IP transfers, etc.)					
Government acquisition processes					
Government purchasing volatility					
Government regulatory burden					
Healthcare costs					
A. Health and safety regulations					
Imports					
Industrial espionage - domestic					
Industrial espionage - foreign					
Intellectual property/patent infringement					
Labor availability/costs					
Material input availability					
Product obsolescence					
Pension costs					
Proximity to customers					
Proximity to suppliers					
R&D costs					
Reduction in commercial demand					
Reduction in USG demand					
Taxes					
Worker/skills retention					
Other (specify here)					
Other (specify here)					
Comments:					
BUSINESS CONFIDEN	TIAL - Per S	Section 70	5(d) of the I	Defense Pr	oduction Act

Next Page

Previous Page					Next Page				
Section 8: Cybersecurity									
Estimate your organization's spending on physical and cyber security:									
Reporting Schedule:		Reco	ord \$ in Thousands, e.g. \$12,0	00.00 = survey input of \$12					
A. 2014		2015	2016	2017	2018				
Cybersecurity Expenditures									
Physical Security Expenditures									
Is your organization aware of Defense Federal Acquisition Regulation Supplem B. Incident Information? http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm	nent (DFARS) 2	52.204-7009, Limitations on the U	Use or Disclosure of Third-Parl	y Contractor Reported Cyber	Yes/No				
1 What group is responsible for administering your organization's compute	r networks? –	Internal Ne	etwork	External Netw	ork				
2 Is the computer or computer network that houses your organization's Connetwork or server?	mmercially Sen	sitive Information* (CSI) connecte	ed to the Internet, either direc	tly or via an intermediary					
3 Estimate the percentage of your organization's CSI stored with external d	iata/cloud stora	age provider(s):							
C. 4 Does your organization either restrict or prohibit your external data/cloud	d storage provi	der(s) from storing CSI outside of	the U.S.?						
Indicate whether your organization typically encrypts CSI data in each of	the following st	tates:	1						
In storage (at rest):	Tr ne	ransmitted across internal etworks		Transmitted outside your organization's networks					
*Privileged or proprietary information which, if compromised through alterat customer/client information, financial information and records, human resou and trademark information, research and development information, regulato	irces informatio	on, intellectual property informati	ion, internal communications,	harm to the organization owning it. manufacturing and production line	This includes information, patent				
Indicate the security measures your organization currently has in place:									
Account Monitoring and Control			Inventory of Authorized/Una	uthorized Software					
Application Software Security			Limitation/Control of Networ	k Ports and Services					
Boundary Defense			Maintenance, Monitoring, &	Analysis of Audit Logs					
Continuous Vulnerability Assessment			Malware Defenses						
D. Controlled Access Based on Need to Know			Penetration Tests and Red Te						
Controlled Use of Administrative Privileges			Secure Configurations on Har						
Data Protection			Secure Configurations of Net	work Devices					
Data Recovery Capability			Secure Network Engineering						
Incident Response and Management			Security Skills Assessments ar	nd Training					
Inventory of Authorized/Unauthorized Devices			Wireless Access Control						
Other (specify here	e)		Other	(specify here)					
1 Is your organization able to detect the theft of, or unauthorized access to			neans?						
2 Does your organization have defined, written protocols in place for respo	inding to a cybe	ersecurity breach?							
Explain:	0040								
Identify any impacts or actions resulting from malicious cyber activity from	n 2013 to prese	ent:		A stimulation and a state laser					
E. IT downtime			Dovised approach to internet	Actions Undertaken					
			Revised approach to internat						
Costs from damage assessment/remediation Significant change in R&D strategy 3 Loss of sales/Business interruption Exit from foreign markets or market segments									
			•						
Exfiltration of CSI data Damage to IT infrastructure			Exit from product or business Major new investment in cyb						
Damage to production capabilities or systems			Other	(specify here)					
Theft of software and/or source code			Other	(specify here)					
Other (specify here	e)		Other	(specify here)					
Note: The FBI encourages recipients to report information concerning suspicious http://www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855 activity, number of people, and type of equipment used for the activity, the nam	or criminal acti 5-292-3937 or e	-mail at <u>CyWatch@ic.fbi.gov</u> . Wh	or the FBI's 24/7 Cyber Watch en available, each report subr	(CvWatch). Field office contacts car	n be identified at e, location, type of				
Comments:									
BUSINESS	CONFIDENTIAL	- Per Section 705(d) of the Defen	se Production Act						

Section 9: Certification

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.A. 1001 (1984 & SUPP. 1197)).

Once this survey is complete, submit it via our Census Bureau web portal at https://respond.census.gov/software survey. Be sure to retain a copy for your records and to facilitate any necessary edits or clarifications.

Organization Name	
Organization's Internet Address	
Name of Authorizing Official	
Title of Authorizing Official	
E-mail Address	
Phone Number and Extension	
Date Certified	
In the box below, 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	