

[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 Information furnished herewith is deemed confidential and will not be published or disclosed except in accordance with Section 705 of the Defense Production Act of 1950, as amended (50 U.S.C App.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 Page](#)[Next Page](#)

Table of Contents

I	Cover Page
II	Table of Contents
III	General Instructions
IV	Glossary
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	Employment
23	Competitiveness
24	Cybersecurity
25	Certification Page

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

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

General Instructions

	<p>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/softwareurvey</p>
A.	<p>If you are not able to download the survey document, at your request, BIS staff will e-mail the Excel survey template directly to you.</p> <p>For your convenience, a PDF version of the survey and required drop-down content is available on the BIS website to aid internal data collection. DO NOT SUBMIT the PDF version of the survey as your response to BIS. Should this occur, your organization will be required to resubmit the survey in the requested Excel format.</p>
B.	<p>Respond to every question. Surveys that are not fully completed will be returned for completion. Use the comment boxes to provide any information to supplement responses provided in the survey form. Make sure to record a complete answer in the cell provided, even if the cell does not appear to expand to fit all of the information.</p> <p>DO NOT CUT AND PASTE RESPONSES WITHIN THIS SURVEY.</p> <p>Survey inputs should be completed by typing in responses or by using a drop-down menu. The use of cut and paste can corrupt the survey template. If your survey response is corrupted as a result of cut and paste responses, a new survey will be sent to your organization for immediate completion.</p>
C.	<p>Do not disclose any classified information in this survey form.</p>
D.	<p>Questions related to the survey should be directed to BIS survey support staff at softwareurvey@bis.doc.gov</p> <p>E-mail is the preferred method of contact.</p> <p>You may also speak with a member of the BIS survey support staff by calling (202) 482-7808.</p>
E.	<p>After completeing, reviewing, and certifying the Excel survey, submit the survey via our Census Bureau web portal:</p> <p>https://respond.census.gov/softwareurvey</p> <p>Do not submit the survey via email.</p>
F.	<p>For questions related to the overall scope of this Industrial Base assessment, contact softwareurvey@bis.doc.gov or:</p> <p>Brad Botwin, Director, Industrial Studies Office of Technology Evaluation, Room 1093 U.S. Department of Commerce 1401 Constitution Avenue, NW Washington, DC 20230</p> <p>DO NOT submit completed surveys to Mr. Botwin's postal or personal e-mail address. All surveys must be submitted via the Census Bureau web portal.</p>

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

[Previous Page](#)[Next Page](#)**Section: Glossary**

Glossary	
Antivirus Scanning Application - Host-based	Antivirus software detects and removes viruses from computers. It also protects against a range of malicious software, including: keyloggers, browser hijackers, Trojan horses, worms, rootkits, spyware, adware, botnets and ransomware.
Computer Operating Systems	A collection of software that manages computer hardware resources and provides common services for computer programs. Source(s): NIST SP 800-152
Data Loss Prevention (DLP)	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, 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
Data Recovery	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, medium, timing, recipient/destination, etc.), within a centralized management framework.
End Point Detection & Response (EDR)	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. 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.
Firewalls - Host/Application Side	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 (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.
Firewalls - Network Side	An inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" 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
Firewalls - Cloud	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 center using an organization's own servers in a platform-as-a-service (PaaS) or infrastructure-as-a-service (IaaS) model. In this structure, the firewall application runs on the virtual servers and protects traffic going to, from, and between applications in the cloud.
Firewalls - Virtualized	A firewall device or service that provides network traffic filtering and monitoring for virtual machines (VMs) in a virtualized environment. As with a traditional network firewall, a virtual firewall inspects packets and uses security policy rules to block unapproved communication between virtual machines.
Firmware	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 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.
Gateway - Modular Internet-of-Things (IoT)	An Internet of Things (IoT) gateway is a physical device or software program that serves as the connection point between the cloud and 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.
Health Management Systems - Network Connected	Health 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 making in health facilities and organizations. Elements may include: Hospitals, clinics, pharmacies, laboratories, billing, insurance providers, and health information exchanges.
Health Systems/Devices - Network Connected	Devices and instruments used 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
Industrial Control Systems - Networked	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 distributed control systems and smaller control systems using programmable logic controllers to control localized processes. Source(s): NIST SP 800-53A Rev. 4

[Previous Page](#)[Next Page](#)**Section: Organization Information**

Provide the following information for this organization:				
A.	Facility/Organization Name			
	Street Address			
	City			
	State			
	Zip Code			
	Website			
	Phone Number			
	Primary CAGE Code			
B.	Is your organization publicly traded or privately held?	Private/Public	If your organization is publicly traded, identify its stock ticker symbol.	
Provide the following information for your parent organization(s), if applicable.				
		Parent Organization #1	Parent Organization #2	
D.	Parent Name			
	Street Address			
	City			
	State/Province			
	Country			
	Postal Code/Zip Code			
C.	Is your parent organization publicly traded or privately held?	Private/Public	If your parent organization is publicly traded, identify its stock ticker symbol.	
Provide the following identification codes, as applicable, for your organization.				
D.	Data Universal Numbering System (DUNS) Code(s)	Harmonized Tariff Schedule (HTS) Code(s)	NAICS (6-digit) Code(s)	
	Find DUNS codes at: http://fedgov.dnb.com/webform	Find HTS codes at: http://hts.usitc.gov	Find NAICS codes at: http://www.census.gov/epcd/www/naics.html	
Indicate if your organization qualifies as any of the following types of business:				
E.	A small business enterprise (as defined by the Small Business Administration)	Yes/No		
	8(a) Firm (as defined by the Small Business Administration)	Yes/No		
	A historically underutilized business zone (HUB Zone)	Yes/No		
	A minority-owned business	Yes/No		
	A woman-owned business	Yes/No		
	A veteran-owned or service-disabled veteran owned business	Yes/No		
Identify the government agencies to which your organization sells information network-related hardware and software products, and associated services:				
F.	Organization	Hardware	Software	Services
	Department of Defense	Yes/No	Yes/No	Yes/No
	Civilian U.S. Government Agencies			
	State Governments			
	Local Governments			
	Regional Government Organizations			
BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act				

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 software-related products that your organization has **developed, manufactured, or marketed** since 2014;
- 2) Indicate those product lines for which your company markets **rebranded** products;
- 3) Identify the types of products that your organization sells where you employ or enlist **third-party companies** to perform servicing and upgrades;
- 4) State the number distinct 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 where 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.

Types of Hardware/Software Technologies	Developed	Manufactured	Marketed	Marketed Rebranded Products Made by Other Companies	Use Third-Party Companies to Procure the Products that This Company Sells	Use Third-Party Companies to Service and Upgrade Products That This Company Sells	Number of Distinct Hardware Products	Estimated Average In-Service Life of Hardware Products Before Replacement - Number of Years	Locations where Enabling Product Software Code is Written	Number of Distinct Software Products	Estimated Average In-Service Life of Software Products Before Replacement - Number of Years	Locations where Enabling Product Software Code is Written
A. Network Infrastructure Devices	Hardware	Hardware	Hardware	Hardware	Hardware	Hardware	1-100 scale	1-25 Drop-Down	Company Sites In U.S.	1-100 scale	1-25 Drop-Down	Company Sites In U.S.
Routers	Software	Software	Software	Software	Software	Software			Company Sites Outside U.S.			Company Sites Outside U.S.
Switches	Both	Both	Both	Both	Both	Both			Company Sites In U.S. & Outside			Company Sites In U.S. & Outside
Gateways - Internet	None	None	None	None	None	None			Contractor Sites in U.S.			Contractor Sites in U.S.
Gateways - Internet Service Provider Grade									Contractor Sites Outside U.S.			Contractor Sites Outside U.S.
Gateways - Cloud									Contractor Sites in U.S. & Outside U.S.			Contractor Sites in U.S. & Outside U.S.
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)												
Firewalls - Host Based												
Firewalls - Network Appliance												
Firewalls - Cloud												
Firewalls - Virtualized												
Web Application Firewalls												
End Point Detection & Response (EDR)												
Deep Packet Inspection (DPI) Appliance												
Security Information and Event Management (SIEM)												
Web Proxies/Content Filtering												
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												
Virtualization Software - Work Station-Based Hypervisor												
Software Defined Networking (SDN) solutions												
Other [Define in Comment Box]												
E. Other Products												
Industrial Control Systems - Networked												
Supervision, 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

Section 1.b - Sources of Software Content & Licensing and Sharing Practices for Information Network Products Designed and Manufactured

Instruction: Using drop-down responses accessed by clicking on the empty response cell, for each technology listed in the left column that was developed, manufactured, or marketed by your organization since 2014--
 1) Indicate whether the software used in your hardware products is internally developed, and indicate whether your software products are based on internally developed software;
 2) State whether your internally developed hardware products incorporate known open-source software, and state whether your internally developed software products contain known open source software;
 3) Specify whether internally developed hardware products contain licensed third-party proprietary software, and state whether internally developed software products contain licensed third-party software;
 4) Specify the types of products for which your company has licensed or contractually shared its network device technologies with other hardware manufacturers and software organizations for the purpose of integrating or embedding it in their products;
 5) Estimate the number of U.S. and non-U.S. companies with which your company has licensed or shared its network technologies since 2014.

Types of Hardware/Software Technologies	Hardware Product Based on Internally Developed Software	Software Product Based on Internally Developed Software	Hardware Internally Developed/ Incorporating Known Open-Source Software	Software Internally Developed/ Incorporating Known Open-Source Software	Hardware Internally Developed/ Incorporating Licensed Third-Party Proprietary Software	Software Internally Developed/ Incorporating Licensed Third-Party Proprietary Software	Licenses/Shares Network Device Technologies	Type of Technology Product Shared	Comment	Licensing/Sharing Number of U.S.-Headquartered Companies	Licensing/Sharing Number of Non-U.S. Headquartered Companies	Comment
A. Network Infrastructure Devices	Yes/No		Yes/No		Yes/No		Yes/No					
Routers								Hardware				
Switches								Software				
Gateways - Internet								Other Intell.Property [Describe in box >]				
Gateways - Internet Service Provider Grade								Other				
Gateways - Cloud												
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)												
Firewalls - Host Based												
Firewalls - Network Appliance												
Firewalls - Cloud												
Firewalls - Virtualized												
Web Application Firewalls												
End Point Detection & Response (EDR)												
Deep Packet Inspection (DPI) Appliance												
Security Information and Event Management (SIEM)												
Web Proxies/Content Filtering												
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												
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												
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

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

Instruction:
 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 XYZ; and
 B) Require XYZ hardware/software to operate; or whether the use of XYZ 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 XYZ or an XYZ affiliate.

Products Sold By Your Organization (Auto-Populate Column Elements from 1a - Block Out Non-Applicable Technologies)	Activities Involving Network Products Utilizing XYZ Hardware/Software Products and Technologies						Identify All Applicable Consulting and Development Activities by Technology				Functional Dependency	Formal Relationships
	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 Consulting Collaboration	Services Consulting Collaboration	Product Development Collaboration	Services Development Collaboration	Products/Services Sold that Require XYZ Technology to Operate; Use is Optional	Types of Formal Technology Partnerships/ Relationships with XYZ since 2014.
A. 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	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												
B. Network Security Devices												
Antivirus Scanning Application - Host Based												
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)												
Firewalls - Host Based												
Firewalls - Network Appliance												
Firewalls - Cloud												
Firewalls - Virtualized												
Web Application Firewalls												
End Point Detection & Response (EDR)												
Deep Packet Inspection (DPI) Appliance												
Security Information and Event Management (SIEM)												
Web Proxies/Content Filtering												
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												
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												
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 1.d - XYZ Technologies Deployed in Company Products & Terms of Technology License

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

	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
A.	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	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 Windows 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:											

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

Section 1.f - Modes of Accessing XYZ Technologies for Product Development-Production & XYZ Technologies Deployed in Company Products - Clones & Counterfeits

Instruction: 1) For each product type listed in the left column, identify the means by which your company gains access to XYZ company technologies for hardware and software integrated into the products that your company designs and manufactures.
 2) For each product type listed in the left column that was sold by your organization from 2014-2018, identify all known to have been subject to unauthorized or counterfeit production.
 3) State whether any of the cloned/counterfeit products utilize your company's device software that employs XYZ technology and services.

	[Auto-Populate from 1c]	Packaged Software Purchased Directly from XYZ Installed by Your Company's Staff	Packaged Software Sold by XYZ Authorized Third-Party Reseller	Packaged Software Downloaded Directly from XYZ Servers	Software Installed at Your Company's Product Manufacturing Facilities by XYZ Employees	Software Installed at Your Product Manufacturing Facilities by XYZ Authorized Third-Party Firms	Cloned/Counterfeit Hardware Products	Cloned/Counterfeits Contain XYZ Technology	Cloned/Counterfeit Software Products	Cloned/Counterfeits Contain XYZ Technology
A. Network Infrastructure Devices	Yes/No	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										
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)										
Firewalls - Host Based										
Firewalls - Network Appliance										
Firewalls - Cloud										
Firewalls - Virtualized										
Web Application Firewalls										
End Point Detection & Response (EDR)										
Deep Packet Inspection (DPI) Appliance										
Security Information and Event Management (SIEM)										
Web Proxies/Content Filtering										
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										
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										
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

Section 1.g - Reasons for Using XYZ Technologies in Company Products

Instruction: Using a ranking of 1-5 (1-being the most important), for each of the XYZ technologies listed in left column identify the top five factors for integrating it into the products sold by your organization. Select "N/A" for the XYZ product/services that your organization does not use.

Reasons for Using XYZ Technology -> -> ->	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 (Use Comment Box)	Other [Explain in Comment Box Below]
A. Types of XYZ Product/Associated Intellectual Property															
XYZ Anti-Virus															
XYZ Internet Security															
XYZ Total Security															
XYZ Small Office Security															
XYZ Professional Services															
XYZ Security Center															
XYZ Expert Services [Penetration, Application Security, Digital Forensics, 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:															

Section 2.a - Embedding of XYZ Software into Manufacturers Information Technology Products

Instruction: Identify all information network hardware and software sold by your company since 2014 that incorporates or otherwise contains embedded XYZ technologies by selecting a response from the drop-down under the "Product Supported by XYZ..." column. Select "None" for hardware products sold by your company that do not contain XYZ technologies. Provide version numbers for each model reported as containing XYZ technologies.

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

Integration of XYZ Technologies in Information Technology 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	
A. Network Infrastructure Devices			Hardware			
Routers			Software			
Switches			Both			
Gateways - Internet			None			
Gateways - Internet Service Provider Grade						
Gateways - Cloud						
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)						
Firewalls - Host Based						
Firewalls - Network Appliance						
Firewalls - Cloud						
Firewalls - Virtualized						
Web Application Firewalls						
End Point Detection & Response (EDR)						
Deep Packet Inspection (DPI) Appliance						
Security Information and Event Management (SIEM)						
Web Proxies/Content Filtering						
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						
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						
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

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 ⇌ ⇌ ⇌

Description of XYZ Technologies in Information Technology 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 Prevention	Network Intrusion Detect.	Network Firewall	Other (Use Comment Box)	Description of Methods for Integrating XYZ Technology into Your Company's Products	Comments
A. 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										
B. Network Security Devices											
	Antivirus Scanning Application - Host Based										
	Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)										
	Firewalls - Host Based										
	Firewalls - Network Appliance										
	Firewalls - Cloud										
	Firewalls - Virtualized										
	Web Application Firewalls										
	End Point Detection & Response (EDR)										
	Deep Packet Inspection (DPI) Appliance										
	Security Information and Event Management (SIEM)										
	Web proxies/content filtering										
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										
	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										
	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.c - Integration/Embedding of XYZ Software into Manufacturers' Information Technology Products

For the different information network products identified on the previous page as incorporating or otherwise containing embedded XYZ technologies, provide:
 1) applicable model numbers;
 2) associated application program interfaces (APIs); and
 3) the software publication certificate associated with XYZ technologies being integrated 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 ⇨ ⇨ ⇨

		Integration of XYZ Software and Services in Information Technology Systems - Program Interfaces/Software Publication Certificates			
Hardware/Software Products Sold By Your Organization that Contain XYZ Technology		#1 Your Company's Product Series/Model Number	Associated Application Program Interfaces (APIs)	Method for Signing Software Publication Certificate	Comments
A.	Network Infrastructure Devices	Auto Populate			
	Routers		Pipeline	Co-Signed	
	Switches		Rest	Signed	
	Gateways - Internet		Shared Memory	Shared Key	
	Gateways - Internet Service Provider Grade		Soap	Not Signed	
	Gateways - Cloud		Other (Use Comment Box)	None	
	Gateway - Modular Internet-of-Things (IoT)			Other (Use Comment Box)	
	Mobile Secure Gateways				
B.	Network Security Devices				
	Antivirus Scanning Application - Host Based				
	Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)				
	Firewalls - Host Based				
	Firewalls - Network Appliance				
	Firewalls - Cloud				
	Firewalls - Virtualized				
	Web Application Firewalls				
	End Point Detection & Response (EDR)				
	Deep Packet Inspection (DPI) Appliance				
	Security Information and Event Management (SIEM)				
	Web Proxies/Content Filtering				
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				
	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				
	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

[Previous Page](#)

[Next Page](#)

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

For the types information technology products identified on the previous page as incorporating or otherwise containing embedded XYZ technologies, provide:

- 1) Model numbers;
- 2) Levels of system access enabled by XYZ software;
- 3) Types of data that can be accessed.

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 Information Technology Systems - System Access & Types of Data				
Hardware Products Sold By Your Organization that Contain XYZ Technology	#1 Your Company's Product Series/Model Number	Types of Data That Can Be Accessed	Levels of System Access Enabled by XYZ Software	Comment
A. Network Infrastructure Devices	Auto-Populate			
Routers		System Configuration	Operating Sys. Data	
Switches		Prop. Busn. Data	Application Data	
Gateways - Internet		System Customization Data	User Data	
Gateways - Internet Service Provider Grade		Application Customization Data	Other (Use Comment Box)	
Gateways - Cloud		Other (Use Comment Box)		
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)				
Firewalls - Host Based				
Firewalls - Network Appliance				
Firewalls - Cloud				
Firewalls - Virtualized				
Web Application Firewalls				
End Point Detection & Response (EDR)				
Deep Packet Inspection (DPI) Appliance				
Security Information and Event Management (SIEM)				
Web Proxies/Content Filtering				
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				
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				
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

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		
Gateway - Modular Internet-of-Things (IoT)		System Services		
Mobile Secure Gateways		Other (Use Comment Box)		
B. Network Security Devices				
Antivirus Scanning Application - Host Based				
Antivirus Scanning Appliances - Enclave Boundary (Gateway-based)				
Firewalls - Host Based				
Firewalls - Network Appliance				
Firewalls - Cloud				
Firewalls - Virtualized				
Web Application Firewalls				
End Point Detection & Response (EDR)				
Deep Packet Inspection (DPI) Appliance				
Security Information and Event Management (SIEM)				
Web Proxies/Content Filtering				
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				
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				
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

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

Instruction: For the information technology products containing XYZ technologies that your company sells:
 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 sold by your organization. Select "None" if your company does not use third-party contractors.
 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 ⇄ ⇄ ⇄

Integration of XYZ Software, Hardware, & Services in Hardware Systems - Product Design, Service and Upgrade Practices					
	#1 Your Company's Product Series/Model Number	Internal Design	Outsourced Design	Third-Party Companies to Service and Upgrade products the company sells	Names of Third-Party Organizations that Service and Upgrade Your Company's Products
A. Network Infrastructure Devices	Auto-Populate				
Routers		Hardware	Hardware	Hardware	
Switches		Software	Software	Software	
Gateways - Internet		Both	Both	Both	
Gateways - Internet Service Provider Grade		None	None	None	
Gateways - Cloud					
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)					
Firewalls - Host Based					
Firewalls - Network Appliance					
Firewalls - Cloud					
Firewalls - Virtualized					
Web Application Firewalls					
End Point Detection & Response (EDR)					
Deep Packet Inspection (DPI) Appliance					
Security Information and Event Management (SIEM)					
Web Proxies/Content Filtering					
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					
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					
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:					

Previous Page

Next Page

Section 3.a - Integration/Embedding of XYZ technologies into Manufacturers Information Technology Products - Telemetry I: Direct Comm, Types of Comm

Instruction:

1) Identify 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.

2) Specify the types of communications that your organization's products send or receive through XYZ networks.

3) State the types of communications alerts/events that are associated with the products marketed by your organization that incorporate XYZ software.

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 ⇨ ⇩ ⇨

	#1 Your Company's Product Series/Model Number	Communicates with XYZ Connected Systems				Types of Communications Received/Sent							Types of Associated Communications Detection Events/Alert Events							
		XYZ Security Network	XYZ Infrastructure	XYZ Affiliate	Other (Use Comment Box)	No XYZ Telemetry	Alerts	Bug Fix Reports	System Operations	Remote Command /Control	System Performance Data	System Updates	User Data	Detection Events, No Data	Detection Events, Sample Hashes	Detection events, Sample Content	Cloud scanning, Sample Sashes	Cloud Scanning, Sample Content	Other Alert, No User Data	Other Alert, User Data
A. Network Infrastructure Devices	Auto Populate																			
Routers			Hardware																	
Switches			Software																	
Gateways - Internet			Both																	
Gateways - Internet Service Provider Grade			None																	
Gateways - Cloud																				
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)																				
Firewalls - Host Based																				
Firewalls - Network Appliance																				
Firewalls - Cloud																				
Firewalls - Virtualized																				
Web Application Firewalls																				
Endpoint Detection & Response (EDR)																				
Deep Packet Inspection (DPI) Appliance																				
Security Information and Event Management (SIEM)																				
Web Proxy/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 Tap PII solutions																				
Data Loss Prevention (DLP)																				
Data Anonymity																				
D. Network Systems																				
Virtual Private Network (VPN)																				
Virtual Private Server (VPS)																				
Virtualization Software - Bare Metal Hypervisor																				
Virtualization Software - Work Station-Based Hypervisor																				
Software Defined Networking (SDN) solutions																				
Other (Define in Comment Box)																				
E. Other Products																				
Industrial Control Systems - Networked																				
Supervisory Control and Data Acquisition (SCADA)-Networked																				
Computer Operating Systems																				
Computer Firmware																				
Systems-On-Chip, Microcontroller Devices																				
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

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

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 ⇄ ⇄ ⇄

		Integration of XYZ Software, Hardware, & Services in Information Technology Systems - Methods for Receiving/Modes for Returning Information									
		Methods for Receiving Updates, Signatures, Instructions					Modes for Returning Information Directly Back to XYZ Company			Comments	
Types of Devices that Communicate		#1 Your Company's Product Series/Model Number	Direct Connection to XYZ	Self-Hosted Mirror	Firmware Update	Other (Use Comment Box)	Direct Connection to XYZ	Self-Hosted Aggregator	Other (Use Comment Box)		
A. Network Infrastructure Devices		Auto-Populate									
	Routers		Hardware								
	Switches		Software								
	Gateways - Internet		Both								
	Gateways - Internet Service Provider Grade		None								
	Gateways - Cloud										
	Gateway - Modular Internet-of-Things (IoT)										
	Mobile Secure Gateways										
B. 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/Content Filtering										
C. 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										
D. Network Systems											
	Virtual Private Network (VPN)										
	Virtual Private Server (VPS)										
	Virtualization Software										
	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										
	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

[Previous Page](#)

[Next Page](#)

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

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:

- 1) Indicators for Passively Detecting XYZ in Information Technology Products
- 2) 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 Products					Report All Indicators Associated With Communications With XYZ Organizations				
	Types of Devices that Communicate Directly	#1 Your Company's Product Series/Model Number	Updates	Signature	Instructions	Other (Use Comment Box)	Internet Protocol Addresses	Domains	Unique Indicators	Other (Use Comment Box)	Comments
A.	Network Infrastructure Devices	Auto-Populate									
	Routers		Hardware								
	Switches		Software								
	Gateways - Internet		Both								
	Gateways - Internet-to-Orbit		None								
	Gateways - Cloud										
	Gateway - Modular Internet-of-Things (IoT)										
	Mobile Secure Gateways										
B.	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/Content Filtering										
C.	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										
D.	Network Systems										
	Virtual Private Network (VPN)										
	Virtual Private Server (VPS)										
	Virtualization Software										
	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										
	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

Section 4 - Practices for Tracking Technologies Used In Hardware & Software Network Products Sold By Your Organization

Identify 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 By Your Organization [Auto-Populate This List Below from 1c]	Maintains a Current List of Third-Party Components Used in its Hardware Products	Maintains a Current List of Third-Party Components Used in its Software Products	Maintains Current List of the Names of Executable Components in its Hardware and Software Products	Keeps Current List of Suppliers of Executable Components Used by Your Company	Maintains a List of Known Vulnerabilities Associated With Third-Party Executable Components	Maintains a List of Known Vulnerabilities Associated With Organization-Owned Executable Components	Notifies purchasers of company products that contain XYZ Technologies	Comment
A.	Network Infrastructure Devices	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	Yes/No	
	Routers								
	Switches								
	Gateways - Internet								
	Gateways - Internet Service Provider Grade								
	Gateways - Cloud								
	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)								
	Firewalls - Host Based								
	Firewalls - Network Appliance								
	Firewalls - Cloud								
	Firewalls - Virtualized								
	Web Application Firewalls								
	End Point Detection & Response (EDR)								
	Deep Packet Inspection (DPI) Appliance								
	Security Information and Event Management (SIEM)								
	Web Proxies/Content Filtering								
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								
	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								
	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

[Previous Page](#)[Next Page](#)**Section 5.a Sales and Balance Sheet**

From 2014-2018 provide your organization's U.S. and non-U.S. sales information.

Reporting Schedule:		Level of Report:				
Record \$ in Thousands, e.g. \$12,000.00 = survey input of \$12		2014	2015	2016	2017	2018
A.	Total Sales, all Customers U.S./Non-U.S. (in \$)					
B.	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 Thousands, e.g. \$12,000.00 = survey input of \$12				
		2014	2015	2016	2017	2018
A.	Net Sales (and other revenue)					
B.	Cost of Goods Sold					
C.	Total Operating Income (Loss)					
D.	Earnings Before Interest and Taxes					
E.	Net Income					
Comments:						
<p>Disclosure of financial information is required for both public and private companies. All financial data is treated as Business Confidential and exempt from Freedom of Information Act (FOIA) requests. Providing BIS with financial information will not result in the public release of your organization's financial data.</p>						
BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act						

[Previous Page](#)

[Next Page](#)

Section 5.b: Research & Development and Capital Expenditures

A.	Does your organization perform Research and Development (R&D)?	Yes/No	If "No", leave part B blank.
----	--	--------	------------------------------

In Part B, record your organization's total R&D expenditures for 2014-2018.

Reporting Schedule:		Record \$ in Thousands, e.g. \$12,000.00 = survey input of \$12				
		2014	2015	2016	2017	2018
B.	1	Total R&D Expenditures				
	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 - 5 (must equal 100%)		0%	0%	0%	0%

In Part C, report your organization's capital expenditures for 2014-2018. If your organization had no capital expenditures in this period enter "0" for each year.

Capital Expenditure Reporting Schedule:		Record \$ in Thousands, e.g. \$12,000.00 = survey input of \$12				
Capital Expenditure Category		2014	2015	2016	2017	2018
C.	1	Total Capital Expenditures				
	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 through 6 must total 100%						

Comments:

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

Section 6: Employment

Record the total number of FTE employees and contractors at this facility for calendar years 2014-2018. Next, estimate the percentage of FTE employees and contractors who are U.S. and non-U.S. citizens. Do not double count personnel who may perform cross-operational roles.

Reporting Schedule:			2014	2015	2016	2017	2018
A.	1	FTE Employees					
	a	FTE Employees - U.S. Citizens (as a % of line 1)					
	b	FTE Employees - non-U.S. Citizens (as a % of line 1)					
	2	FTE Contractors					
	a	FTE Contractors - U.S. Citizens (as a % of line 2)					
	b	FTE Contractors - non-U.S. Citizens (as a % of line 2)					

List the top five countries (other than the U.S.) from which your facility has non-U.S. citizen workers (employees or contractors), and identify the number of each type of visa or green card holder associated with each country.

Country	H-1B	H-2B	F-1	Green Card	O-1	Other

Comments:

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

Section 7: Competitiveness

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.

Issue	2014 to Present		2019-2023		Explain
	-Yes/No-	Rank	-Yes/No-	Rank	
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 CONFIDENTIAL - Per Section 705(d) of the Defense Production Act

[Previous Page](#)[Next Page](#)**Section 8: Cybersecurity**

Estimate your organization's spending on physical and cyber security:					
A. Reporting Schedule:		Record \$ in Thousands, e.g. \$12,000.00 = survey input of \$12			
		2014	2015	2016	2017
Cybersecurity Expenditures					
Physical Security Expenditures					
B. Is your organization aware of Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information? http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm					Yes/No
1 What group is responsible for administering your organization's computer networks?		Internal Network		External Network	
2 Is the computer or computer network that houses your organization's Commercially Sensitive Information* (CSI) connected to the Internet, either directly or via an intermediary network or server?					
3 Estimate the percentage of your organization's CSI stored with external data/cloud storage provider(s):					
C. 4 Does your organization either restrict or prohibit your external data/cloud storage provider(s) from storing CSI outside of the U.S.?					
5 Indicate whether your organization typically encrypts CSI data in each of the following states:					
In storage (at rest):			Transmitted across internal networks		Transmitted outside your organization's networks
*Privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organization owning it. This includes customer/client information, financial information and records, human resources information, intellectual property information, internal communications, manufacturing and production line information, patent and trademark information, research and development information, regulatory/compliance information, and supplier/supply chain information.					
Indicate the security measures your organization currently has in place:					
Account Monitoring and Control				Inventory of Authorized/Unauthorized Software	
Application Software Security				Limitation/Control of Network Ports and Services	
Boundary Defense				Maintenance, Monitoring, & Analysis of Audit Logs	
Continuous Vulnerability Assessment				Malware Defenses	
Controlled Access Based on Need to Know				Penetration Tests and Red Team Exercises	
Controlled Use of Administrative Privileges				Secure Configurations on Hardware	
Data Protection				Secure Configurations of Network Devices	
Data Recovery Capability				Secure Network Engineering	
Incident Response and Management				Security Skills Assessments and Training	
Inventory of Authorized/Unauthorized Devices				Wireless Access Control	
Other		(specify here)		Other (specify here)	
1 Is your organization able to detect the theft of, or unauthorized access to, Commercially Sensitive Information by cyber means?					
2 Does your organization have defined, written protocols in place for responding to a cybersecurity breach?					
Explain:					
Identify any impacts or actions resulting from malicious cyber activity from 2013 to present:					
Impacts Experienced			Actions Undertaken		
IT downtime				Revised approach to international partnerships	
Costs from damage assessment/remediation				Significant change in R&D strategy	
Loss of sales/Business interruption				Exit from foreign markets or market segments	
Exfiltration of CSI data				Exit from product or business line	
Damage to IT infrastructure				Major new investment in cybersecurity	
Damage to production capabilities or systems				Other (specify here)	
Theft of software and/or source code				Other (specify here)	
Other		(specify here)		Other (specify here)	
Note: The FBI encourages recipients to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at http://www.fbi.gov/contact-us/field . CyWatch can be contacted by phone at 855-292-3937 or e-mail at CyWatch@ic.fbi.gov . When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting organization, and a designated point of contact.					
Comments:					
BUSINESS CONFIDENTIAL - Per Section 705(d) of the Defense Production Act					

[Previous Page](#)

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