Next Page

OMB Control Number: 0694-0119
Expiration Date: September 30, 2015

U.S. Biomedical Industry Cyber Security Assessment

SCOPE OF ASSESSMENT

The U.S. Department of Commerce, Bureau of Industry and Security (BIS), Office of Technology Evaluation (OTE), in coordination with other key federal cyber partners, is conducting a pilot industrial base assessment of the effect of cyber security threats on the U.S. biomedical industry. The purpose of this survey is to provide the U.S. Government with a baseline understanding of the challenges and business-related impacts attributed to cyber security threats. Additionally, the data collected will provide an overview of the preventive measures taken by organizations in this critical industrial sector.

The ability of biomedical companies to protect their Commercially Sensitive Information (CSI) is vital to the industry's continued competitiveness and overall success in the global marketplace. Through the results of this assessment, both government and industry will be better informed when developing effective policy responses and investment strategies to mitigate the growing cyber security threat, and ensure the ability of the biomedical industry to support critical national security and civilian requirements.

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 Information furnished herewith is deemed confidential and will not be published or disclosed except in accordance with Section 705 of the Defense Production Act of 1950, as amended (50 U.S.C App.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

Not withstanding 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 12 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information to BIS Information Collection Officer, Room 6883, Bureau of Industry and Security, U.S. Department of Commerce, Washington, D.C. 20230, and to the Office of Management and Budget, Paperwork Reduction Project (OMB Control No. 0694-0119), Washington, D.C. 20503.

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

Previous Page Next Page

Table of Contents

Previous Page Next Page

Section I	GENERAL INSTRUCTIONS
A.	Your organization is required to complete this survey using an Excel template, which can be downloaded from the U.S. Department of Commerce, Bureau of Industry and Security (BIS) website: http://www.bis.doc.gov/biomedsurvey At your request, survey support staff will e-mail the Excel survey template directly to your organization. For your convenience, a PDF version of the survey is available on the BIS website to aid internal data collection. DO NOT submit the PDF version of your organization's response.
B.	Respond to every question. Surveys that are not fully completed will be returned for completion. Use 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 the information. **DO NOT COPY AND PASTE RESPONSES WITHIN THIS SURVEY.** Survey inputs should be made manually, by typing in responses or by use of a drop-down menu. The use of copy and paste can corrupt the survey template. If your survey response is corrupted as a result of copy and paste responses, a new survey will be sent to you for immediate completion.
C.	**Do not disclose any classified information in this survey form.**
D.	If information is not available from your organization's records in the form requested, you may furnish estimates.
E.	Questions related to this Excel survey should be directed to: Mark Crawford, Senior Trade & Industry Analyst, (202) 482-8239 Erika Maynard, Trade & Industry Analyst, (202) 482-5572
F.	Upon completion, review, and certification of the Excel survey, transmit the survey via e-mail attachment to: biomedsurvey@bis.doc.gov Be sure to retain a copy for your records.
G.	For questions related to the overall scope of this industrial base assessment, contact: Brad Botwin, Director, Industrial Studies Office of Technology Evaluation, Room 1093 U.S. Department of Commerce 1401 Constitution Avenue, NW Washington, DC 20230 To contact Mr. Botwin, call (202) 482-4060. DO NOT submit completed surveys to Mr. Botwin's postal or personal e-mail address; all surveys must be submitted electronically to biomedsurvey@bis.doc.gov

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

Previous Page Next Page

Section II	Definitions
Term	Definition
Advanced Persistent Threat (APT)	Refers to a persistent type of cyber attack designed to evade an organization's present technical and process countermeasures. APTs are specifically designed to bypass firewalls, intrusion detection systems, and anti-malware programs.
Adversary Command and Control (C2)	A cyber attack that utilizes a compromised or infected computer system that then allows the hacker to control and direct additional attacks or actions against other systems and or networks from that compromised system.
Air Gapped	Type of network secured by keeping it isolated from other local networks and the Internet.
Application Blacklisting	A network administration practice used to prevent the execution of undesirable programs by placing them on an unauthorized list.
Application Whitelisting	A network administration practice used to prevent unauthorized programs from running by placing approved applications on an executable list.
Botnet	A collection of Internet-connected programs communicating with other similar programs in order to perform tasks.
Cloud Storage	A service model in which data is maintained, managed, and backed up remotely and made available to users over a network.
Commercially Sensitive Information (CSI)	Privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organization owning it.
Criminal Syndicates	Network or organization of actors engaged in criminal and nefarious attacks on information systems.
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Cyber Security	Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
Cyber Security Service Provider	An individual or organization that provides cyber security services that include but are not limited to: network security engineering, network security monitoring, defense and testing, cyber security training, and policy development, as well as responding to, and remediation of, cyber incidents.
Cyber Terrorism	The politically motivated use of computers and information technology to cause severe disruption or widespread fear in society.
Data Loss Prevention (DLP)	A system that is designed to detect potential data breach/data ex-filtration transmissions and prevent them by monitoring, detecting, and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage). In data leakage incidents, sensitive data is disclosed to unauthorized personnel either by malicious intent or inadvertent mistake.
Denial of Service (DoS)	A denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users.
Electronic Watermarking	Data-embedding and watermarking algorithms embed text, binary streams, audio, image, or video in a host audio, image, or video signal. The embedded data are perceptually inaudible or invisible to maintain the quality of the source data.
Extranet	Extranet is a computer network that allows controlled access from the outside for specific business or educational purposes. Extranets are extensions to, or segments of, private intranet networks that have been built in many corporations for information sharing and ecommerce. Most extranets use the Internet as the entry point for outsiders, a firewall configuration to limit access, and a secure protocol for authenticating users.
External Storage	External storage is all addressable data storage that is not currently in your company's networks main storage or memory.

Previous Page Next Page

Section II	Definitions *(continued)*
Term	Definition
Full Time Equivalent (FTE) Employees	Employees who work for 40 hours in a normal work week. Convert part-time employees into "full-time equivalents" by taking their work hours as a fraction of 40 hours.
Hacktivist	A computer hacker whose activity is aimed at promoting a social or political cause.
Honeypot	A decoy computer system for trapping hackers or tracking unconventional or new hacking methods. Honeypots are designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet. Multiple honeypots can be set on a network to form a honeynet.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
Infrastructure as a Service	Provides the computing infrastructure, physical or (quite often) virtual machines and other resources like virtual-machine disk image library, block and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks etc. Examples: Amazon EC2, Windows Azure, Rackspace, Google Compute Engine.
Intranet	Intranet is the generic term for a collection of private computer networks within an organization. An intranet uses network technologies as a tool to facilitate communication between people or work groups to improve the data sharing capability and overall knowledge base of an organization's employees. Intranets utilize standard network hardware and software technologies like Ethernet, Wi-Fi, TCP/IP, Web browsers and Web servers.
Intrusion Detection System (IDS)	A device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.
Intrusion Prevention System (IPS)	A network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.
Joint/Multi Tenancy	Joint/Multi Tenancy is an information network operating model in which two or more organizations use shared infrastructure, including network hardware and software platforms, and/or information storage assets to facilitate more effective collaboration and to achieve higher operational and cost efficiencies. This business model can include the provisioning of business and research software tools to enable companies and organizations to operate on common systems to facilitate cross organizational collaboration and business activities. And, it can enable shared access to data sets, projects, and research programs on a controlled basis.
Lone Wolf	Person who acts alone in computer network exploitation activity.
Nation State	Actor(s) with allegiance to and tasked by a sovereign state.
National Institute of Standards and Technology (NIST) Cyber Security Framework	The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. See http://www.nist.gov/cyberframework/ for more information.
Password Sniffing	The electronic eavesdropping or monitoring of existing network traffic to capture passwords as they cross a network.
Penetration Test	An attack on a computer system with the intention of finding security weaknesses and potentially gaining access to the systems, its functionality, and data.
Personally Identifiable Information (PII)	Any information about an individual maintained by an organization, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.
Phishing	The attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.
Platform as a Service	Provides computing platforms which typically includes operating system, programming language execution environment, database, web server, etc. Examples include: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, and Apache Stratos.
Portable Electronic Devices	Devices with the capability of wireless or local area network (LAN) connectivity. These include, but are not limited to: laptop computers with wireless capabilities, cellular/personal communication system devices, audio/video/data recording or playback devices, scanning devices, remote sensors, messaging devices, personal digital assistants (PDAs) (for example, Blackberries, Palm Pilots, Pocket PCs), and two-way radios.
Protected Health Information (PHI)	Any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.
Social Media	Social media includes personal and professional websites, blogs, chat rooms, and bulletin boards; social networks, such as Facebook, LinkedIn and Twitter; video-sharing sites such as YouTube; and e-mail.
Software as a Service	Model(s) organizations are provided with access to application softwares often referred to as on-demand softwares. The service provider handles installation, setup and running of the application. Examples include: Google Apps and Microsoft Office 365.
Vulnerability Scanner	A computer program designed to assess computers, computer systems, networks, or applications for weaknesses.
Web Application Firewall (WAF)	An appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (CSS) and SQL injection. By customizing the rules to your application, many attacked can be identified and blocked.

Previous Page Next Page

Section 1.a: Organization Information

A. Provide the following information for your organization:

Organization Name	
Facility Name (if applicable)	
Street Address	
City	
State	
Zip Code	
Website	
Phone Number	

B. Provide the following information for your parent organization, if applicable.

Organization Name	
Street Address	
City	
State	
Country	
Postal Code/Zip Code	

C. Does this survey response capture the operations of your whole organization or that of an individual business unit/division?

Note: All data in this survey response must be reported at the same organizational level.

D. Is your organization publicly traded or privately held? | Stock Symbol, if applicable:

E. Identify and rank in descending order all entities that directly or indirectly own or have beneficial ownership of five percent or more of your organization:

	Entity Name	Percentage of Financial Interest Held	Street Address	City	State	Country
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

F. Point of contact for this survey:

Name	Title	Phone Number	E-mail Address	State	Country

G. Point of contact for internal cyber security programs:

Name	Title	Phone Number	E-mail Address	State	Country

Comments:

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

Previous Page Next Page

Section 1.b: Organization Information *(continued)*

A. Identify your organization's primary business line and provide a brief description. If your organization has additional business lines list them on lines 2-5 and provide a brief description.

		Business Line (drop-down)	Describe (write-in)
1	Primary Business Line	Distribution/brokerage/reseller/retail	
2	Additional Business Line	Production	
3	Additional Business Line	Research and development	
4	Additional Business Line	Raw materials provider	
5	Additional Business Line	Testing/evaluation	

B. Does your organization participate in the following biomedical segments? If yes, provide a brief description.

		Participate? (drop-down)	Describe (write-in)
1	Pharmaceutical		
2	Biotechnology		
3	Medical Devices		
4	Diagnostics		
5	Other		

Comments:	

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

Previous Page Next Page

Section 2: Financial Information

A. Provide your organization's Total Net Sales and Total R&D Expenditures for 2014.

Note: Record in $ Thousands, e.g. $12,000.00 = survey input $12

	Source of Data:	
	Reporting Schedule:	
		2014
1	Total Net Sales (and other revenue)*	
2	Total R&D Expenditures*	

*As reported on your income statement

B. Provide your organization's Total Operating Expenditures, Information Security Related Expenditures and Cyber Security Related Expenditures for 2013 and 2014 and provide an estimate for 2015 and 2016.

Note: Record in $ Thousands, e.g. $12,000.00 = survey input $12

		Source of Expenditure Data:				
		Reporting Schedule:				
			2013	2014	2015 (estimate)	2016 (estimate)
1	Total Operating Expenditures*					
2	Information Security Related Expenditures					
3	Cyber Security Related Expenditures					

*As reported on your income statement

C. Have recent cyber incidents across the marketplace cause your organization to increase its information security budget?

Comments:

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

Previous Page Next Page

Section 3: Employment Information

A.	Provide your organization's Total Full-Time Equivalent (FTE) employees for 2015. Then, estimate the number of your FTEs that work on cyber security-related activities.		
		Source of Data:	
		Reporting Schedule:	
			2015
	1	Total Full-Time Equivalent (FTE) Employees	
	2	FTEs that work on cyber security-related activities	
B.	Estimate the number of on-site and external FTE contractors supporting cyber security-related activites at your organization.		
	1	On-Site Contractors	
	2	External Contractors	

C.	For FTE employees and on-site contractors that work on cyber security-related activities, estimate the percent that are U.S. and non-U.S. citizens.			
			FTE Employees	On-Site Contractors
		Total:		
	1	U.S. Citizens (as a percent of Total)		
	2	Non-U.S. Citizens (as a percent of Total)		
	3	Unknown Citizenship (as a percent of Total)		
		Lines 1-3 must sum to 100%	**0%**	**0%**

Comments:	

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

Previous Page Next Page

Section 4: Customers

A.	Does your organization sell to commercial customers?	

If yes,list your organization's top ten commercial customers based on 2014 sales, ranked in descending order. Provide the customer name and their location (city, state, country).

	Customer Name (write-in)	City (write-in)	State (drop-down)	Country (drop-down)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

B.	Does your organization sell directly or indirectly to the United States Government (USG)?	

If yes, list your organization's top ten USG customers by 2014 sales, ranked in descending order. Provide the USG customer name, the USG Department/Agency, and location (city, state).

	USG Customer Name (write-in)	USG Department/Agency (write-in)	City (write-in)	State (drop-down)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Comments:	

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

Previous Page Next Page

Section 5: Facilities

Does your organization have multiple facilities (including leased and owned facilities)?	

If yes, identify all U.S. and non-U.S. facilities. Provide the location of the facility and indicate its primary operation. If your organization has more than 25facilities contact BIS staff or e-mail biomedsurvey@bis.doc.gov for further instructions.

	Facility Name (write-in)	Location			Operation	
		City (write-in)	State (drop-down)	Country (drop-down)	Facility Primary Operation (drop-down)	Specify Additional Detail or "Other" Operation (write-in)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						

Comments:	

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

Previous Page Next Page

Section 6: Commercially Sensitive Information (CSI)

	Does your organization have defined, structured methods for actively protecting the following types of Commercially Sensitive Information (see definitions)?		
	Commercially Sensitive Information (CSI):		Yes/No (drop-down)
A.	Customer/client information		
	Financial information and records		
	Human resources information/employee data		
	Information subject to export control regulations (EAR and/or ITAR)		
	Intellectual property related information		
	Internal communications including negotiation points, merger and acquisition plans, and/or corporate strategy		
	Manufacturing and production line information		
	Patent and trademark information		
	Regulatory/compliance information		
	Research and development (R&D) related information		
	Supply chain and sourcing information		
	Other	(specify here)	

Comments:	

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

Previous Page

Next Page

Section 7.a: Network Information

A.	Indicate who is responsible for your organization's internal IT networks:	
B.	Indicate who is responsible for your organization's external IT networks:	

C. If your organization has any external providers that are responsible for its IT networks, provide the name and type of provider. Next, indicate their location and select the service(s) they provide to your organization.

	External IT Service Provider (write-in)	Type of Provider (drop-down)	City (write-in)	State (drop-down)	Country (drop-down)	Service Provided 1 (drop-down)	Service Provided 2 (drop-down)	Service Provided 3 (drop-down)	Service Provided 4 (drop-down)	Service Provided 5 (drop-down)
1		Telecommunications Carrier				Switches/Routers				
2		National Consulting/Operations Manager				Network Servers				
3		Regional or Local IT services company				IT Software				
4		Network Security				Telephony				
5		Other				System Administration				
6						Patches/Updates				
7						System scanning				
8						Enterprise Firewall/Intrusion Protection				
9						Overall Network Security				
10						Cloud Services (operate over Internet)				
11						Data Storage				
12						Other				
13										
14										
15										

Comments:	

Previous Page Next Page

Section 7.b: Network Information *(continued)*

A.	Does your organization's internal and/or external network(s) connect to the Internet? If yes, provide the external facing IP Address(es) and public domain name(s) below.		Internal Network (drop-down)	External Network (drop-down)
	External Facing IP Addresse(es):		Public Domain Name(s):	
	1		1	
	2		2	
	3		3	
	4		4	
	5		5	
B.	Does your organization have joint/multi tenancy agreements related to the use of CSI data in the following (see definitions)?			
	1	Infrastructure as a Service		
	2	Platform as a Service		
	3	Software as a Service		
	Comments:			

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

Previous Page Next Page

Section 7.c: Network Information *(continued)*

A.	Does your organization encrypt its CSI data?			
B.	Estimate the percent of CSI data your organization encrypts:			
C.	Does your organization encrypt CSI data in storage (at rest)?			
	If yes, at what level of encryption?			
	Explain:			
D.	Does your organization encrypt data transmitted across internal networks?		If yes, at what level of encryption?	
	Does your organization encrypt data meant for transmission outisde of your organization's networks?		If yes, at what level of encryption?	
	Explain:			
E.	Does your organization allow remote access to CSI data?			
	If yes, how is CSI data remotely accessed?			
F.	Does your organization electronically watermark any of its CSI data (see definitions)?			
	Comments:			

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

Previous Page Next Page

Section 7.d: Network Information *(continued)*

Identify where your organization purchases and/or acquires software, hardware, and portable electronic devices (PEDs). Select all that apply:

			Directly from Manufacturer (drop-down)	Authorized Distributor (drop-down)	Other Distributor (drop-down)	Authorized Reseller (drop-down)	Other Reseller (drop-down)	Build Internally (drop-down)	Retail (drop-down)	Other Source (drop-down)	Other (write-in)
A.	Software										(specify here)
	Hardware										(specify here)
	Portable Electronic Devices (PEDs)										(specify here)
	Other	(specify here)									(specify here)

Identify the party responsible for purchasing and/or acquiring software, hardware, and portable electronic devices (PEDs) for your organization. Select all that apply:

			Internal Staff (drop-down)	Consultant/External Contractor (drop-down)	Other (drop-down)	Other (write-in)
B.	Software					(specify here)
	Hardware					(specify here)
	Portable Electronic Devices (PEDs)					(specify here)
	Other	(specify here)				(specify here)

Comments:	

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

Previous Page

Next Page

Section 8.a: Data Storage

A.	Does your organization operate its own data center in the U.S.?	
	If yes, how many data centers does your organization operate in the U.S.?	
B.	Does your organization operate its own data center outside the U.S.?	
	If yes, how many data centers does your organization operate outside the U.S.?	
C.	Is your organization's CSI data stored in locations outside the U.S. by a parent organization and/or an affiliated subsidiary? If yes, complete D and E below.	
D.	Estimate the percent of your organization's CSI data that is stored in locations outside the U.S. by a parent organization or an affiliated subsidiary:	

E. List the name of each parent organization and/or affiliated subsidary that stores your CSI data at locations outside the U.S., their location, and the county(ies) where the CSI data is stored.

	Name of Parent Organization/Affiliated Subsidiary (write-in)	Relationship (drop-down)	City (write-in)	State (drop-down)	Country (drop-down)	Country where CSI data is stored (drop-down)	Country where CSI data is stored (drop-down)	Country where CSI data is stored (drop-down)	Country where CSI data is stored (drop-down)	Country where CSI data is stored (drop-down)
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Comments:	

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

Previous Page Next Page

Section 8.b: Data Storage *(continued)*

A.	Does your organization use an external cloud service or external data storage provider?	
	If yes, does your organization restrict or prohibit your external cloud service or external data storage provider(s) from storing CSI data outside of the U.S.?	

B. If your organization has external cloud service and/or external data storage provider(s), list the name, type, and location of each provider. For each identified provider, indicate whether or not they store your organization's CSI data outside of the U.S. If your organization's CSI data is stored outside of the U.S., indicate the country(ies) where your CSI data is stored.

	Name of Provider (write-in)	Type of Provider (drop-down)	City (write-in)	State (drop-down)	Country (drop-down)	Is CSI data stored outside U.S.? (drop-down)	Country where CSI data is stored (drop-down)	Country where CSI data is stored (drop-down)	Country where CSI data is stored (drop-down)	Country where CSI data is stored (drop-down)
1		External Cloud Service Provider								
2		External Data Storage Provider								
3		Both								
4										
5										
6										
7										
8										
9										
10										

C.	Estimate the percent of your organization's CSI data that is stored with each of the following:	External Cloud Service Provider	External Data Storage Provider

D.	Does your organization internally back-up any of its CSI data that is stored with an outside provider?	
E.	Does your organization operate an internal cloud to store CSI data?	
	If yes, estimate the percent of your organization's CSI data that is stored on your organization's internal cloud:	
F.	In the next year, will your organization's demand for cloud storage increase, decrease, or remain the same?	

Comments:	

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

Previous Page Next Page

Section 9.a: CSI Data Exchanges

A.	As a condition of doing business with a non-U.S. entity, has your organization ever been requested or required to grant access to your organization's CSI data?	
B.	As a condition of doing business with a non-U.S. entity, has your organization ever been requested or required to grant access to your organization's networks?	

C. If your organization answered yes to either Question A or B, list the name of the non-U.S. entity and their location. Then, indicate if access was either requested or required as a condition of doing business, and the response of your organization. Finally, if CSI data was requested and/or required as a condition of doing business select the CSI type(s).

	Name of non-U.S. Entity (write-in)	Location		Access/Response				Type of Commercially Sensitive Information (CSI)											
		City (write-in)	Country (drop-down)	Access to organization's network requested or required? (drop-down)	Organization response regarding network (drop-down)	Access to CSI data requested or required? (drop-down)	Organization response regarding CSI data (drop-down)	Customer/client information	Financial information and records	Human resources information/ employee data	Information subject to export control regulations	Intellectual property related information	Internal communications	Manufacturing and production line information	Patent and trademark information	Research and development (R&D) related information	Regulatory/ compliance Information	Supply chain and sourcing information	Other
1				Requested	Complied with Requirement														
2				Required	Complied with Request														
3				No	Did not comply with requirement														
4					Did not comply with request														
5					Did not comply with requirement, still conducted business with entity														
6					Did not comply with request, still conducted business with entity														
7					Partially complied with requirement, conducted business with entity														
8					Partially complied with request, conducted business with entity														
9					Other														
10																			

Comments:

Previous Page

Next Page

Section 9.b: CSI Data Exchanges *(continued)*

Does your organization exchange your CSI data with any external organizations (including suppliers, customers, subcontractors, non-U.S. owned parent company, etc.) or individuals on a recurring basis for collaboration, production, design, and/or research and development?

If yes, list the names of all the external organizations with which you exchange CSI data and identify their location. Next, indicate what types of CSI data you exchange with the organization.

A.

	Name of External Organization (write-in)	Type of External Organization (drop-down)	Location			CSI Type											
			City (write-in)	State (drop-down)	Country (drop-down)	Customer/client information	Financial information and records	Human resources information/ employee data	Information subject to export control regulations	Intellectual property related information	Internal communications	Manufacturing and production line information	Patent and trademark information	Research and development (R&D) related information	Regulatory/ compliance Information	Supply chain and sourcing information	Other
1		Supplier															
2		Customer															
3		Subcontractor															
4		Non-U.S. Owned Parent Company															
5		U.S. Owned Parent Company															
6		Other															
7																	
8																	
9																	
10																	
11																	
12																	
13																	
14																	
15																	
16																	
17																	
18																	
19																	
20																	
21																	
22																	
23																	
24																	
25																	

Comments:

Previous Page Next Page

Section 10.a: Cyber Security Policy and Programs

A.	Does your organization have a written IT acceptable use policy?		
	If yes, how frequently is it reviewed and/or updated?		
	Explain:		
B.	Does your organization employ a defined set of written cyber security practices and procedures?		
	If yes, how frequently is it reviewed and/or updated?		
	Explain:		
C.	Does your organization provide cyber security/IT training to employees?		
	Explain:		
D.	What percent of employees receive cyber security training provided by your organization?		
	How frequently is this training required?		
E.	What percent of your organization's internal contractors receive cyber security training provided by your organization?		
	How frequently is this training required?		
F.	Are employees at your organization provided with written instructions on how to best inform management of suspected or known cyber security incidents?		
	Explain:		

			Yes/No (drop-down)	Explain (write-in)
G.	Does your organization limit employee access to CSI data via the following controls:			
	Principle of least privilege			
	Separation of duties			
	Rotation of duties			
	Time of day restrictions			
	Role or Rule set based access control			
	Other	(specify here)		

Comments:	

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

Previous Page Next Page

Section 10.b: Cyber Security Policy and Programs *(continued)*

A.	Does your organization face any of the following challenges when protecting its operations against cyber security risks? If yes, explain.			
	Challenges		Yes/No (drop-down)	Explanation (write-in)
	Inadequate and/or timely threat information			
	Insufficient budget resources			
	Lack of trained cyber security personnel			
	Low prioritization of cyber security by senior organizational leadership			
	Poor collaboration on cyber security issues across business lines			
	Lack of buy-in from employees to adhere to cyber security policies and practices			
	Limited knowledge of cyber security issues and risks			
	Other	(specify here)		
B.	Does your organization currently have a cyber security insurance policy?			
	If yes, explain.			
	Comments:			

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

Previous Page Next Page

Section 11: Cyber Security Services

A.	Identify the primary provider(s) of your organization's cyber security services:	

B. Identify all external cyber security providers, their location, and select the service(s) they provide to your organization.

	Name of External Cyber Security Provider (write-in)	City (write-in)	State (drop-down)	Country (drop-down)	Service Provided 1 (drop-down)	Service Provided 2 (drop-down)	Service Provided 3 (drop-down)	Service Provided 4 (drop-down)	Service Provided 5 (drop-down)
1					Network defense				
2					Network monitoring				
3					Training				
4					Response and remediation				
5					Network engineering				
6					Other				
7									
8									
9									
10									

Comments:	

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

Previous Page Next Page

Section 12: Critical Controls

A. Identify which of the following cyber security controls your organization actively employs by identifying whether they are performed by internal staff, contractors, both, or neither.

Cyber Security Control		Performed by: (drop-down)
Account Monitoring and Control		Internal staff
Application Software Security		Contractors
Boundary Defense		Both
Continuous Vulnerability Assessment and Remediation		Neither
Controlled Access Based on the Need to Know		
Controlled Use of Administrative Privileges		
Data Protection		
Data Recovery Capability		
Incident Response and Management		
Inventory of Authorized and Unauthorized Devices		
Inventory of Authorized and Unauthorized Software		
Limitation and Control of Network Ports, Protocols, and Services		
Maintenance, Monitoring, and Analysis of Audit Logs		
Malware Defenses		
Penetration Tests and Red Team Exercises		
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers		
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches		
Secure Network Engineering		
Security Skills Assessment and Appropriate Training to Fill Gaps		
Wireless Access Control		
Other	(specify here)	
Other	(specify here)	

B. Does your organization incorporate a honeypot mechanism within its IT infrastructure (see definitions)?

Explain:

Comments:

Previous Page Next Page

Section 13.a: Cyber Threats and Incidents

A.	On a scale from 1 (very low threat) to 5 (very high threat) indicate the degree to which each of the following types of actors represent a threat to your organization's CSI data:		
	Commercial competitors (domestic)		5 - Very high threat
	Commercial competitors (foreign)		4 - High threat
	Cyber criminals		3 - Moderate threat
	Hacktivists		2 - Low threat
	Insider threats		1 - Very low threat
	Nation-state actors		
	Other	(specify here)	

B.	Are there any specific nation-state actors that pose a high threat to your organization? If yes, specify below.	
	Country 1	
	Country 2	
	Country 3	
	Country 4	
	Country 5	

C.	How concerned is your organization about each of the following cyber incidents?		
	Incident Type		Concern
	Targeted attack		1 – Not at all concerned
	Network intrusion		2 – Slightly concerned
	Distributed Denial of Service (DDoS) attack		3 – Somewhat concerned
	Phishing attacks		4 – Moderately concerned
	Other	(specify here)	5 – Extremely concerned
	Other	(specify here)	

D.	Rate the importance of each of the following elements as part of your organization's overall cyber security plan.		
	Protecting against the loss of income/market share		1 - Not at all important
	Protecting against the loss/compromise of CSI data		2 - Slightly important
	Complying with legal/regulatory requirements		3 - Somewhat important
	Protecting organization reputation/brand		4 - Moderately important
	Ensuring continuity of business operations		5 - Extremely important
	Other	(specify here)	
	Other	(specify here)	
	Other	(specify here)	

Comments:	

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

Previous Page Next Page

Section 13.b: Cyber Threats and Incidents *(continued)*

Indicate whether or not your organization or security provider is able to detect and/or prevent the following types of malicious cyber incidents.

If yes, estimate the number of malicious cyber incidents prevented and/or detected for 2013, 2014, and 2015 (to date).

	Malicious Cyber Incident		Able to detect/prevent incident?	Total Number of Malicious Cyber Incidents		
				2013	2014	2015 (to date)
A.	Adversary Command and Control (C2)		Detect			
	Being the recipient of spear phishing messages		Prevent			
	Being fraudulently represented as a sender of phishing messages		Both			
	Bots/zombies within the organization		Do not know			
	Denial of service attacks		Not able to detect or prevent			
	Exploit of client web browser					
	Exploit of DNS server					
	Exploit of user's social network profile					
	Exploit of wireless network					
	Extortion or blackmail associated with threat of attack or release of stolen data					
	Insider abuse of Internet access or e-mail					
	Laptop or mobile hardware theft or loss					
	Malware infection					
	Password sniffing					
	System penetration by outsider					
	Theft of or unauthorized access to intellectual property by cyber means					
	Theft of or unauthorized access to intellectual property by means other than cyber					
	Theft of or unauthorized access to Personally Identifiable Information (PII)					
	Theft of or unauthorized access to Protected Health Information (PHI)					
	Unauthorized access or privilege escalation by insider					
	Other	(specify here)				
	Other	(specify here)				
	Other	(specify here)				

Comments:	

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

Previous Page Next Page

Section 14: Loss Related to Cyber Attacks

A. During the last 36 months, has your organization experienced any of the following global market anomalies possibly associated with the compromise of CSI data? If yes, explain.

Anomaly		Experienced? (drop-down)	Explain (write-in)
Emergence of new domestic competition			
Emergence of new foreign competition			
Appearance of similar products or activities (potentially on an accelerated schedule)			
Appearance of access to internal knowledge of pending mergers and acquisitions or other business ventures			
Appearance of access to internal knowledge of supply agreements, pricing, or other business activity			
Competitor patents product immediately before your organization intended to do so			
Compromised negotiation talking points or sensitive internal data			
Departure of key employee(s)			
Party(ies) inquiring about or investing in your organization before or after a series of cyber activity is detected			
Party(ies) interested in purchasing your organization before or after a series of cyber activity is detected			
Other	(specify here)		
Other	(specify here)		
Other	(specify here)		

B. During the last 36 months, has your organization experienced any of the following impacts due to malicious cyber activity? If yes, indicate the impact level and explain.

Impact		Yes/No (drop-down)	Impact Level (drop-down)	Explain (write-in)
User idle time and lost productivity because of downtime or systems performance delays		Yes	High	
Disruption to normal operations because of system availability problems		Yes	Medium	
Damage or theft of IT assets and infrastructure		Yes	Low	
Incurred cost of damage assessment and remediation			Not Applicable	
Business interruption				
Exfiltration of CSI data				
Theft of personnel information				
Damage to software and/or source code				
Theft of software and/or source code				
Damage to company production capabilities or systems				
Destruction of information asset				
Reputation loss, market share, and brand damages				
Other	(specify here)			
Other	(specify here)			
Other	(specify here)			

Comments:	

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

Previous Page Next Page

Section 15: Cyber Threats Focused on Employees

A.	Does your organization have a written employee conduct policy related to social media (LinkedIn, Facebook, Twitter, etc.)?	
	Explain:	
B.	Does your organization allow access to social media (LinkedIn, Facebook, Twitter, etc.) and personal e-mail websites via company networks and/or devices?	
	Explain:	
C.	Have any of your employees reported being approached on social media (LinkedIn, Facebook, Twitter etc.) for CSI related information?	
	Explain:	
D.	Does your organization have a bring your own device policy?	
	Explain:	
E.	Do employees take Portable Electronic Devices (PEDs) that contain CSI information to foreign countries?	
	Explain:	
F.	Does your organization have a policy related to employees bringing PEDs that contain CSI information to foreign countries?	
	Explain:	
G.	Does your organization have a policy to check PEDs when employees return from foreign travel?	
	Explain:	
H.	Have any of your employees reported the theft or potential compromise (unauthorized access) of their PEDs while traveling to foreign countries? If yes, explain and include the location(s) of the incident(s).	
	Explain:	

Comments:	

Previous Page Next Page

Section 16: Advanced Persistent Threat (APT)

A.	Can your organization detect an Advanced Persistent Threat (see definitions)?		
B.	During the past 36 months, has your organization been subject to an Advanced Persistent Threat (APT)?		
C.	How many separate APT-related incidents did your organization face over the past 36 months?		
D.	Identify the impacts your organization experienced from APT-related incidents (select all that apply):		
	IT downtime		
	Cost of damage assessment and remediation		
	Business interruption		
	Exfiltration of CSI data		
	Theft of personnel information		
	Damage to IT infrastructure		
	Damage to software and/or source code		
	Theft of software and/or source code		
	Damage to company production capabilities or systems		
	Destruction of information asset		
	Other	(specify here)	
	Other	(specify here)	
	Comments:		

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

Previous Page Next Page

Section 17: Collaboration and Partnership

A. Does your organization belong to any formal or informal government or industry cyber security related information sharing or related groups?

If yes, list the name and type of group(s) your organization participates in and provide a brief description of its activities.

	Group Name	Type of Group	Description of Activities
1		Industry	
2		Government (local, state, federal)	
3		Non-profit organization	
4		Academic/university	
5		Other	
6			
7			
8			
9			
10			

B. Does your organization utilize sector specific cyber security best practices or standards? If yes, explain.

Explain:

C. Is your organization aware of the National Institute of Standards and Technology (NIST) Cyber Security Framework (see definitions)?

Explain:

D. Does your organization employ any of the NIST Cyber Security Framework's recommended controls?

Explain:

E. Does your organization have a U.S. Government contract that requires you to have certain cyber security practices in place?

Explain:

F. Do outside organizations or vendors supply your organization with the latest information regarding cyber-related threats, intelligence, and/or indicators of compromise?

Explain:

G. Does your organization rely on the U.S. Government for the latest information regarding cyber-related threats, intelligence, and/or indicators of compromise?

Explain:

Comments:

Previous Page Next Page

Section 18.a: United States Government (USG) Assistance and Outreach

A.	Does your organization know what government agencies to contact to report and/or obtain assistance related to cyber security incidents?	
B.	Has your organization identified any points of contact at any government agencies to report and/or obtain assistance related to cyber security incidents?	
C.	Has your organization ever contacted the government to report and/or obtain assistance related to cyber security incidents? If yes, identify the reason for contact and explain.	

	Agency Name		Reason for Contact (drop-down)	Explain (write-in)
1	Defense Security Service (DSS)		To report incident(s)	
2	Department of Homeland Security (DHS)		To obtain assistance	
2.a	Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)		To report incident(s) and obtain assistance	
2.b	United States Computer Emergency Readiness Team (US-CERT)			
3	Federal Bureau of Investigation (FBI)			
4	Local or State Law Enforcement			
5	National Institute of Standards and Technology (NIST)			
6	United States Secret Service			
7	Other	(specify here)		
8	Other	(specify here)		
9	Other	(specify here)		
10	Other	(specify here)		

Comments:	

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

Previous Page Next Page

Section 18.b: United States Government (USG) Assistance and Outreach *(continued)*

	Would your organization be interested in the following:		
A.	1	Receiving additional cyber security related information and best practices from the USG	
	2	Collaborating with other companies for cyber security related best practices	
	3	Providing cyber security related information, assistance, and/or training to other members of your industry	
	4	Receiving cyber security related information, assistance, and/or training to other members of your industry	
	5	Participating in a cyber security related mentoring program with another company	
	6	Participating in USG cyber security related technical advisory panels/working groups	

Comments:	

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

Previous Page

Section 19: 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))

Organization Name	
Organization's Internet Address	
Name of Authorizing Official	
Title of Authorizing Official	
Email 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