Department of Homeland Security
National Protection and Programs Directorate

Paperwork Reduction Act

IT SCC - Questions for SMBs.[1]

This is a two-part questionnaire. Questions 1-11 are intended for CEO, while the remaining portion requires technical information and should be filled out by CISO and IT staff.

Respondent Contact Information

Name (Last, First) and Email: _____

1. What is the organization's core business function?

- ☐ 511210 - Software Publishers
- ☐ 518210 - Data Processing, Hosting, and Related Services
- ☐ 519130 - Internet Publishing and Broadcasting and Web Search Portals
- ☐ 519190 - All Other Information Services
- ☐ 541511 - Custom Computer Programming Services
- ☐ 541512 - Computer Systems Design, Development and Integration Services
- ☐ 541513 - Computer Facilities Management Services
- ☐ 541519 - Other Computer Related Services
- ☐ Public Federal
- ☐ Public State
- ☐ Local Municipality
- ☐ Other _____

2. What are the primary industry sectors your organization is supporting, i.e. what type of customers constitute your primary market segment?

Private:	
☐ Chemical Facilities	☐ Food and Agriculture

[1] Last update: May 1, 2017

☐ Commercial Facilities ☐ Communications ☐ Critical Manufacturing ☐ Dams ☐ Defense Industrial Base ☐ Emergency Services ☐ Energy ☐ Financial Services	☐ Healthcare and Public Health ☐ Information Technology ☐ Nuclear Reactors, Materials and Waste ☐ Transportation ☐ Water and Wastewater ☐ Non-profit/Not for profit ☐ Academic ☐ Other _____
Public: ☐ Federal ☐ State	 ☐ Local Municipality ☐ Other _____

3. Size of the company:

a. What is your estimated annual revenue?

☐ < $1M ☐ $1M-$5M ☐ $5M-$10M ☐ $10-$20M ☐ $20-$30M	☐ $30-$38.5M ☐ $40M - $50M ☐ $50M - $100M ☐ $100M - $500M

b. How many employees work at your organization?

☐ No Employees ☐ Under 20 ☐ 20-99 ☐ 100-499 ☐ 500-749 ☐ 750-999	☐ 1,000-1,499 ☐ 1,500-2,499 ☐ 2,500-4,999 ☐ 5,000-9,999 ☐ 10,000 or more

c. Years in business _____

4. Safeguarded assets (cyber-relevant)

a. Types of critical assets as related to the mission space

☐ Personally Identifiable Information (PII) (e.g., customer lists, consumer contact information)
☐ Protected Health Information (PHI) (e.g., including medical records, other health data collected via apps and wearables, medical device data)
☐ Financial/Account Information (e.g., credit card records, transactional data, or in providing a service to business customer)
☐ Personal Confidential Information (e.g., private email, employer records, etc.)
☐ Corporate Confidential Information (e.g., corporate email, business-sensitive documentation)
☐ Intellectual Property (IP) (e.g., trade secrets, copyrightable materials, patents, designs)

- ☐ SCADA/ICS (industrial control systems)
- ☐ Customer-facing Website
- ☐ Business Application Servers and/or Transaction Systems
- ☐ Embedded Systems (e.g., Building Controls, Medical Devices, etc.)
- ☐ End points (e.g., PCs, Tablets, Smartphones)
- ☐ IT Infrastructure Systems (e.g., DNS servers, data centers)
- ☐ Encryption Keys
- ☐ Other _____
- ☐ Not Applicable

b. What are your primary cyber impact of concerns as related to these assets?

☐ PII or PHI Loss ☐ IP Loss ☐ Financial Loss ☐ Reputation Loss	☐ Availability of Data/Information ☐ Integrity of Data/Information ☐ Operational Functionality (ICS or Embedded Systems) ☐ Mission Disruption/Denial of Service ☐ Other _____

c. What is the perceived value of your top assets?

☐ < $1M ☐ $1M-$5M ☐ $5M-$10M ☐ $10-$20M ☐ $20-$30M ☐ $30-$40M	☐ $40M - $50M ☐ $50M - $100M ☐ $100M - $500M ☐ $500M - $1B ☐ More than $1B ☐ Unknown

5. Cybersecurity capabilities:

a. What are current cybersecurity capabilities of your organization?

- ☐ Dedicated staff/department handling internal cybersecurity issues
- ☐ No stand-alone department, combined with other functions
- ☐ Mostly Outsourced (established relationship with a third party)
- ☐ Blended approach with a smaller portion of cybersecurity responsibilities outsourced
- ☐ Ad hoc, no specifically identified internal or external cybersecurity support

b. What is the approximate IT share relative to revenue? _____%

c. What is the cybersecurity share in the overall IT budget? _____%

6. How does your organization rank cybersecurity and information security relative to other priorities?

a. Relative ranking as compared with other aspects of the core business objectives. Please assign a rank from 1 to 7 to the following areas:

_____ Attracting New Customers
_____ Retaining Existing Customers
_____ Cybersecurity
_____ Financing
_____ Physical Security
_____ Attracting Talent
_____ Compliance with the Regulations

b. Importance of cybersecurity for your business

☐ Cyber security is HIGHLY IMPORTANT for my business
☐ Cyber security is IMPORTANT for my business
☐ Cyber security is SOMEWHAT IMPORTANT for my business
☐ Cyber security is NOT IMPORTANT for my business

7. NIST Cybersecurity Framework (NIST CSF):

a. Is your organization familiar with the NIST CSF? ☐ Yes ☐ No

b. If yes, is your organization IMPLEMENTING the NIST CSF?

☐ Yes
☐ Yes, but in conjunction with other frameworks, standards and practices

c. If no,

☐ Are you using some other framework, standards or practices
☐ Currently not using any

8. If your organization is aware of the NIST CSF, but not using it, what are the barriers to its implementation?

☐ Lack of implementation guidance
☐ Lack of specific technical information sources
☐ NIST CSF is complex and hard to understand
☐ Organization lacks technical expertise to support implementation
☐ Insufficient information on the cost burden of the NIST CSF implementation
☐ Insufficient budget
☐ Cost-effectiveness considerations
☐ Other_____
☐ Using some other standards/framework instead

9. What other cybersecurity practices, standards and procedures are being implemented by your organization as part of the cyber risk management?

☐ CCS CSC ☐ COBIT 5 ☐ NIST SP 800-53 ☐ ISA 62443 ☐ ISO/IEC 27001/27002	☐ CIS Critical Security Controls (formerly SANS Top 20) ☐ PCI Payment Card Industry Data Security Council Standard ☐ Other _____ ☐ We do not use any cybersecurity frameworks

10. What information sources are you relying on for the cybersecurity best practices?

- ☐ Getting Started for Business - *https://www.us-cert.gov/ccubedvp/smb*
- ☐ MS-ISAC Cyber Security Toolkit - *https://msisac.cisecurity.org/toolkit/*
- ☐ FCC Small Biz Cyber Planner 2.0 - *https://www.fcc.gov/cyberplanner*
- ☐ Cyber Resilience Review (CRR) - *https://www.us-cert.gov/ccubedvp/assessments*
- ☐ US-CERT Resource List – *https://www.us-cert.gov/sites/default/files/c3vp/smb/Top_SMB_Resources.pdf*
- ☐ NIST SMB Information Security Guide: The Fundamentals - *http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf*
- ☐ Other (Specify) _____
- ☐ None of the above

11. What do you think the likelihood is that your organization will experience an incident in the next 2-3 years?

☐ Very Unlikely	☐ Unlikely	☐ Likely	☐ Very Likely

12. If your organization is using NIST CSF framework, please answer the set of questions below.

a. How long has your organization been using the NIST CSF? _____years

b. What element(s) of the NIST CSF have been implemented in your organization? (check all that apply)

☐ **Framework Core**
- ☐ Identify Categories/subcategories
- ☐ Protect Categories/subcategories
- ☐ Detect Categories/subcategories
- ☐ Respond Categories/subcategories
- ☐ Recover Categories/subcategories

☐ **Framework Profiles**
- ☐ Profile provided by sector/subsector
- ☐ Profile specific to our organization

☐ **Framework Implementation Tiers**
☐ **Other_____**

c. What were the factors driving NIST CSF adoption?

☐ NIST CSF is considered a best practice
☐ Federal contract required it
☐ Non-federal contract required it
☐ Business partner required it
☐ Other _____

d. Is NIST CSF implemented in a segment of organization or throughout the entity?

☐ Segment	☐ Throughout the organization	☐ Not Implemented

e. To the best of your ability, please determine the value the NIST Cybersecurity Framework has provided to these aspects of your organization

	Affect			
Possible Value	**Positive**	**Neutral**	**Negative**	**Non-Applicable**
Characterize the Cybersecurity Framework's affect with regard to:	-	-	-	-
Understanding or managing cybersecurity risk				
Managing or fulfilling cybersecurity requirements				
Prioritizing the relative importance of cybersecurity requirements or activities				
Determining areas for improvement and developing plans to achieve improvements				
Reducing risk				

f. What was the approximate cost of the NIST CSF implementation:

I. Staff Time/Total Cost _____$ thousand
II. Acquisitions (software and hardware)/Total Cost _____$ thousand

g. What was the impact of the NIST CSF implementation on the information security (cost savings or change in practices, both short-term and long-term)?

I. Total cost savings _____$ thousand
II. Change in practices _____$ thousand

h. What was the impact on operations (cost savings or change in practices, short-term and long-term)?

I. Total cost savings _____$ thousand
II. Change in practices _____$ thousand

13. How many endpoints/hosts and servers does your organization have on the network?

I. Endpoints/hosts/terminals _____
II. Servers _____

14. What portion of the systems are you most concerned about?

☐ 10% or less ☐ 10 - less than 25% ☐ 25 - less than 50%	☐ 50% - less than 75% ☐ 75% or more ☐ Prefer not to disclose ☐ Do not know

15. Do you have an on-file asset inventory, data flow and core network diagram with access points documented? Please select Yes or No for each document below:

a. Asset Inventory	☐ Yes	☐ No
b. Data Flow	☐ Yes	☐ No
c. Core Network Diagram	☐ Yes	☐ No
d. Access Points Documented	☐ Yes	☐ No
e. Security Architecture Diagram	☐ Yes	☐ No

16. How is physical access to the assets managed?

☐ All physical locations of assets are documented, physical access is strictly monitored
☐ Location of SOME assets is documented, limited management of physical access
☐ Other_____

17. How is remote access to the assets managed?

☐ Established usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed
☐ Connections are implemented through managed interfaces
☐ Controls have been implemented to protect all communication and control network (technology) assets
☐ Systems are monitored to detect unauthorized local, network, and remote connections.
☐ Other _____

18. How is patching and remediation managed?

☐ Ad Hoc reactive patching and remediation

☐ Standard managed program with regular updates in place
☐ Established relationship with an outside product and service providers
☐ Other _____

19. Are system changes and incidents tracked?

a.	Incidents Tracked	☐ Yes	☐ No
b.	System Changes Tracked	☐ Yes	☐ No

20. If a cyber incident were to occur, how would it be handled?

☐ Ad Hoc response
☐ Cyber response plan or disaster response plan in place with POCs, roles and responsibilities identified
☐ Established relationship with an outside product and service providers

21. Overall, how would you rate your relative cybersecurity maturity of your organization compared to your competitors?

☐ New to market; novice experience
☐ Beginner; beginning to develop cybersecurity processes
☐ Intermediate; some processes are in place
☐ Mature; processes are used and improved regularly

22. In which of the following cybersecurity focus areas could your organization improve (select all that apply)?

☐ Access and identity management
☐ Vulnerability management
☐ Antivirus/malware management
☐ Endpoint security
☐ Network security
☐ Intrusion detection and protection
☐ Secure development and testing practices
☐ Encryption management (key storage, rotation, protocol selection)
☐ Incident management and data breach response
☐ Training and awareness