# Council of Better Business Bureaus

*Information on Current and Future States of Cybersecurity in the Digital Economy*

Request for Information
National Institute for Standards and Technology
September 9, 2016

## About the Council of Better Business Bureaus

The Council of Better Business Bureaus (CBBB) is the umbrella organization for the local, independent BBBs in the United States, Canada and Mexico, as well as home to its national and international programs on dispute resolution, advertising review, and industry self-regulation.

Like BBBs, CBBB is dedicated to fostering honest and responsive relationships between businesses and consumers - instilling consumer confidence and advancing a trustworthy marketplace for all.

For more than 100 years, Better Business Bureau has been helping people find businesses, brands and charities they can trust. In 2015, people turned to BBB more than 172 million times for BBB Business Reviews on more than 5.3 million businesses and Charity Reports on 11,000 charities, all available for free at bbb.org.

## Contact at the Council of Better Business Bureaus

For additional information about content in this document please contact:

Bill P. Fanelli, CISSP
Chief Security Officer

703-247-9408
bfanelli@council.bbb.org

## Table of Contents

## Executive Summary

Small and Mid-sized Businesses (SMBs) with fewer than 500 employees comprise over 99% of the employer firms in the U.S. and produce almost half of the non-farm GDP. SMBs with fewer than 20 workers still make up almost 90% of U.S. employers. BBB believes that SMBs must take a leading role in cybersecurity to maintain consumer trust in the marketplace. In addition, SMBs are often important links in the supply chain to larger companies and therefore have a direct impact on our nation's critical infrastructure.

BBB has identified a gap in the ability of SMBs to operationalize cybersecurity practices appropriate to their businesses. This observation is derived from our leadership role in the SMB marketplace as well as longstanding relationships with governmental entities, including DHS, NIST, FBI and FTC, and the many major corporations affiliated with BBB as National Partners.

Feedback from BBB Accredited Businesses through our nationwide system of local BBBs indicates that there is a strong and growing awareness of the NIST Cybersecurity Framework (CSF) which is being accelerated by the roll out of BBB's CSF-based "5 Steps to Better Business Cybersecurity" training through BBBs in North America. The 5-Steps training applies the five Functions of the CSF – Identify, Protect, Detect, Respond and Recover – to a fictional small business case study.

Despite some evidence of expanding CSF awareness among SMBs, they continue to exhibit a much lower level of CSF adoption than the broader marketplace. Through feedback from training and frequent surveys of our membership, BBB observes that the two largest barriers to CSF adoption for SMBs are clear direction and cost of implementation. BBB is actively working to accelerate awareness and promote adoption. Feedback from BBB National Partners, all of whom are major U.S. corporations, many of whom are thought leaders in cybersecurity, indicates that shortcomings in cybersecurity implementation in SMBs are of concern to larger businesses as well, since SMBs form many of the links in their supply chain. (For a list of BBB National Partners see: https://www.bbb.org/council/the-national-partner-program/our-partners/.)

To address the above concerns, BBB developed a Public Awareness and Education campaign based on the 5-Steps training described above, to be implemented with the support of sponsors such as cybersecurity product and cybersecurity insurance vendors. Furthermore, the BBB initiative is as applicable to the Critical Infrastructure IT Sector based on the applicability of SMB approaches to small government entities such as town and village governments. We are exploring ways to partner with these communities, as well.

In addition to our 5-Steps training, BBB is working with cybersecurity vendors to map their products to the CSF to make the path to adoption clearer for SMBs. BBB is exploring ways to expand this mapping to include both policies and specific configurations under particular threat-based use cases. Our comprehensive SMB approach also includes consideration of cybersecurity insurance to mitigate residual risk.

Other areas where BBB is actively engaged in cybersecurity initiatives include:

- White House "Lock Down Your Login" Campaign
  - BBB participated in the development of this messaging with the White House and NCSA. BBB is a sponsor organization for the launch in late September.
- DHS Cyber Incident Data and Analysis Working Group (CIDAWG)
  - BBB is participating in the CIDAWG to define a cyber incident data and analysis repository (CIDAR) to be shared among contributors, cybersecurity insurance companies, cybersecurity product vendors and researchers. BBB has offered to host a pilot effort when appropriate.

## Topics

BBB will provide input on the following topics referenced in the Commission's RFI:

- Public Awareness and Education (targeted at SMBs)
- Cybersecurity Insurance
- Critical Infrastructure Cybersecurity – IT Sector

## Public Awareness and Education

BBB's response focuses primarily on RFI topic Public Awareness and Education - specifically, cybersecurity awareness training targeted at SMBs.

BBB developed cybersecurity awareness training based on the NIST Cybersecurity Framework (CSF) targeted at SMBs. Our "5 Steps to Better Business Cybersecurity" training, developed in collaboration with the National Cyber Security Alliance (NCSA), will be made available through BBBs throughout North America.

Several local BBBs are hosting 5-Steps training events in support of National Cybersecurity Awareness Month (NCSAM) in 2016. BBB is partnering with cybersecurity and cybersecurity insurance vendors to sponsor many more events through 2017 targeted at SMBs starting with our membership of almost 400,000 BBB Accredited Businesses.

The BBB 5-Steps training is part of the larger BBB Cybersecurity Program. 5-Steps builds awareness of the CSF and makes it relevant to SMBs. In the longer term, BBB is working on ways to provide more specific guidance to SMBs on how to secure their businesses to foster trust in the marketplace with consumers and business customers.

## Cybersecurity Insurance

As part of the program described above, BBB is crafting a complete risk management schema for SMBs to deploy which will incorporate cybersecurity insurance, as appropriate, to help mitigate residual risk.

## Critical Infrastructure – IT Sector

The Department of Homeland Security (DHS) is assigned as Sector-Specific Agency (SSA) for the Critical Infrastructure IT Sector. DHS National Protection and Programs Directorate (NPPD) coordinates the IT Government Coordinating Council (IT GCC). The IT GCC comprises Federal, State, and local governments as providers of IT services that support public health, safety and confidence needs of citizens, businesses, and employees.

BBB Education and CSF adoption guidance will be targeted at SMBs. Many small local government entities operate within very similar environments and constraints as small businesses. Therefore, within many States, local governments and related organizations will be effectively served by BBB resources developed for SMBs. Examples include executive government offices at the town and village level, as well as water and wastewater utilities, municipal police departments and local schools.

## Challenges and Approaches

## Current and Future Trends and Challenges

### *Current Trends*

BBB sees a current trend of emerging awareness of the CSF in the SMB community. We are currently conducting research on this topic and early results indicate approximately 30% of the BBB Accredited Business community is aware of the CSF. In our data, SMBs are equally as aware or more aware of the CSF as they are of security frameworks that have been in existence for several decades such as COBIT (Control Objectives for Information and Related Technologies) and the ISO/IEC 27000-series published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

### *Future trends*

We predict an increase in awareness continuing into the future, accelerated by our 5-Steps initiatives. In addition to in-person events at the local BBB level, we plan to introduce a web-based component to achieve the scale necessary for the desired reach.

### *Challenges*

BBB sees the primary challenge in this area as adoption of the CSF by SMBs. While SMBs report increasing levels of awareness of the CSF, the data suggests that implementation is still minimal.

Since the CSF was initially targeted at and adopted by critical infrastructure stakeholders, SMBs tend to view it as the purview of much larger businesses. SMBs will need much more specific guidance on the implementation and utility of the CSF for smaller entities to drive its widespread adoption. The BBB's role has been to translate the CSF for SMBs.

### *Progress on Challenges*

BBB is making progress on these challenges on several fronts. In the near term, BBB is partnering with private sector cybersecurity product vendors to map their products to the CSF. These materials will then be made available as part of vendor sponsored 5-Steps events to SMBs.

## Promising Approaches to Address the Challenges

### *BBB Training*

BBB sees great promise in accelerating the uptake of the CSF into the SMB community particularly through our 5-Steps training, but this is only a necessary first step. Awareness must lead to adoption to have any measureable effect. BBB is researching approaches to facilitate CSF adoption particularly within SMBs. In the meantime, our 5-Steps training expands and prepares the market for adoption.

### *BBB Partnering with Industry*

BBB is currently partnering with cybersecurity vendors to map their products to the CSF. In the longer term, the BBB is pursuing clear, concise instructions for SMB deployment of the CSF. These same vendors will map their products to these instructions along with specific configuration instructions for a compliant implementation.

BBB is similarly partnering with cybersecurity insurance vendors to provide policy offerings to SMBs who implement the recommended CSF adoption practices.

## Addressing the Challenges in the Next Two Years

### *Continue and Expand 5-Steps Training*

BBB recommends continuing and expanding on the promising approaches described above. In the near term this starts with the 5-Steps awareness training. BBB seeks additional support in our efforts to be coordinated with our Federal Government partners described below to support our mutual outreach efforts to the SMB community. In the future, BBB expects to address emerging security topics for SMBs, such as collecting and securing biometric data for authentication and fraud detection, and deploying and securing Internet of Things (IoT) devices.

### *Advance CSF Adoption*

In the longer term, BBB requests cooperation from DHS and NIST in researching approaches to foster CSF adoption in SMBs.

## Addressing the Challenges in the Next Ten Years

### *Recognition*

The BBB recommends development of a system to recognize SMBs who demonstrate compliance with CSF adoption and hence enhance their trust with consumers and other customers in the marketplace and building robust private/public partnerships which include organizations in the nonprofit sector with expertise and outreach capabilities at both the national and grassroots level.

## Economic Incentives

### *Tax Incentives for SMBs*

BBB data indicates the two largest barriers to CSF adoption in SMBs are clear direction and cost. BBB is actively advancing approaches to providing direction. The Federal Government is uniquely positioned to offer tax incentives to SMBs to foster wide deployment of cybersecurity controls once a clear approach can be defined.

### *Government-Private Sector Coordination*

In addition to our private partnerships described above, BBB has many existing strong partnerships with the Federal Government through other programs that we will to leverage as part of the BBB Cybersecurity Program. We request the Committee's support of these efforts.

### *NIST*

BBB is working with the NIST Small Business Corner (SBC) office to share resources and coordinate activities. NIST is targeting SMBs of 500 employees and below. BBB's outreach effort is focused on companies with 1 to 50 employees.

### *FBI/InfraGard*

BBB is working with an existing FBI public/private partnership, InfraGard, to help recruit cybersecurity professionals in our research into CSF adoption approaches.

### *DHS*

BBB is engaging DHS in their charter under Executive Order 13636, Improving Critical Infrastructure Cybersecurity, to disseminate the CSF to leverage their existing activities to identify adoption approaches.

## Role of Government

### *Procurement Incentives*

BBB encourages the Federal Government to explore opportunities to include incentives in procurement vehicles as clear guidance becomes available for SMBs to follow. Since the CSF is being promulgated as a voluntary program by DHS, care should be exercised to provide incentives rather than simply making compliance mandatory.

## Performance Measures

### *Track Incidents*

The Federal Government can include where appropriate performance measures in the Quality Assurance Surveillance Plan (QASP) of contracts with SMBs. Two performance measures that could drive desired behavior would be:

- Count of cybersecurity incidents within the subcontractor environment that affected delivery on the contract
- Count of cybersecurity incidents within the Federal Government IT environment that are traceable to SMB contractors

## Complexity of Terminology

## NIST CSF provides Lexical Bridge between Cybersecurity Experts and Management

### *CSF Success Based in Accessibility*

BBB observes that much of the appeal of the CSF to SMBs is its utility as a management tool both for non-technical managers and IT specialists. At the CSF Function level, managers can see where expenditures track to cyber investments in a way that they can grasp. At the same time, CSF employs a more security-specific lexicon to provide clear direction to IT and cyber professionals at the sub-category level. The CSF mapping of Functions to Categories and Sub-Categories provides cyber experts a channel to communicate resource requirements and associated benefits to management in terminology that is digestible. Similarly, management can provide resources and direction in Functional areas that IT and cyber experts can then allocate to specific Sub-Categories and implement.

### *Continue and Expand Training based on CSF*

Continued and expanded awareness training based on the CSF will greatly enhance conversations about cybersecurity between business managers and technologists. For SMBs, it is particularly important to implement CSF terminology throughout the vendor marketplace, since SMBs are more likely to seek IT and cyber expertise from external vendors.