ASPEN TECH
POLICY HUB

POLICY

Improving Small Business Cybersecurity Practices Through Procurement Policy

Big Security for Small Business

MATT SIEVERS

MATTHEW SCHROEDER

EXECUTIVE SUMMARY

Small businesses that provide products and services to state, local, tribal, and territorial (SLTT) governments often fail to adhere to strong cybersecurity practices, leaving their data vulnerable and their digital networks open to attack. This policy brief provides a framework that SLTT governments can adopt to modify their procurement policies to improve vendor cybersecurity. It includes a template for a Cybersecurity Plan with 12 measures businesses can follow to improve their cybersecurity with minimal investment in time and money. By punishing non-compliant vendors with the termination of their contracts, SLTT governments can improve the overall cybersecurity posture of businesses operating across their jurisdictions, while also ensuring that their data is more secure.

RECOMMENDATION

Small businesses face a difficult challenge: they are expected to uphold the same strong cybersecurity standards as large enterprises but lack similar resources. High cost and a lack of expertise are the top reasons small businesses cite when asked why they do not adopt stronger cybersecurity practices. Small businesses also are frequently targeted by cyber criminals. These challenges increase the risks of data breaches that could lead to business failure.

When a small business's digital network is breached, it risks exposing data about a range of partners, including customers, business partners, and government entities they serve. Small businesses need strong cybersecurity, but understandably do not prioritize investing money and time to implement necessary practices when there is little demand for security from customers.

THE ASPEN INSTITUTE

We recommend that SLTT governments incentivize better cybersecurity practices by modifying their procurement policies to require vendors competing for contracts to present a Cybersecurity Plan, a commitment to adhere to a set of defined cybersecurity practices. Such plans can take many forms, but we recommend that they be based on well-established frameworks such as the NIST Cybersecurity Framework (CSF).

Such a requirement would be effective at protecting businesses, governments, and consumers while minimizing cost and administrative burden. While the policy we are recommending would be limited to small businesses competing for SLTT contracts, this regulation could help transform the norms and cybersecurity preparedness of all businesses.

✓ Our Template Cybersecurity Plan, modeled off a successful DoD program and based on the CSF, is specifically scoped for small businesses and reduces the costs of compliance by focusing on 12 measures in seven key areas: roles and responsibilities, account management, authentication and password management, data backups and disposal, vulnerability management, and incident response and recovery.

★ This policy would minimize enforcement costs by using a self-certification model. Companies attest their compliance, ideally through a secure web portal. A set of contracts are audited through established SLTT processes, validating actual practices. Falsified statements can lead to contract termination.

To support compliance with this policy, SLTTs should consider providing small businesses with relevant support resources, such as educational materials, cost reimbursement, tax credits, fee waivers, and/or professional assistance.

ASPEN TECH POLICY HUB

POLICY

ABOUT THE HUB

The Aspen Tech Policy Hub is a Bay Area policy incubator, training a new generation of tech policy entrepreneurs. We take tech experts, teach them the policy process, and support them in creating outside-the-box solutions to society's problems.

The Aspen Institute
2300 N St. NW, Suite 700
Washington, DC 20037
202 736 5800

THE ASPEN INSTITUTE