Testimony of Angela Dingle

On behalf of

Women Impacting Public Policy

Submitted to the

House Small Business Committee

"Foreign Cyber Threats: Small Business, Big Target"

July 6, 2016

Good afternoon. Chair Chabot, Ranking Member Velazquez and distinguished Members of the Committee, thank you for the opportunity to testify. My name is Angela Dingle. I am the President and CEO of Ex Nihilo, a women-owned small business, based in Washington, DC that provides cyber security, governance and risk management services to government agencies.

I am here today representing Women Impacting Public Policy (WIPP) where I serve as Chair of its Education Foundation. WIPP is a national nonpartisan public policy organization advocating on behalf of its coalition of 4.7 million businesswomen including 78 business organizations.

First, let me thank the Committee for holding this hearing. WIPP is appreciative of the bipartisan efforts of this Committee to advance the agenda of women entrepreneurs including accessing capital, accessing federal markets, and providing a business friendly environment.

Few topics are as timely as today's hearing: the proliferating danger of cyber threats and their impact on the small business community. Witnesses today will share statistics that portray a ubiquitous threat facing businesses of all sizes—the most devastating impact on smaller firms. In a hearing earlier this year, the Committee noted, "The outcome of an attack can be catastrophic for small business owners because many firms are unable to recover from the loss of their intellectual property or resources."[1] That conclusion is borne out by findings from the National Cyber Security Alliance that 60% of small businesses will close within six months of a cyber attack.[2]

Narrowing the focus, businesses that work with the federal government are an additional security risk as the U.S. Government's research data and engineering specifications are of high value to individuals, companies, and governments across the world. Due to increasing privacy requirements and recent cyber-attacks, the Department of Defense (DOD) has responded by implementing new technical and contractual requirements for contractors doing business with them.

My testimony will focus on these new regulations and their potential to threaten the nearly 75,000 women-owned firms engaged with the federal government. WIPP is particularly concerned about the significant cost associated with these requirements and their potential

---

[1] House Committee on Small business, (2016, April 20). Hearing Memo: Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks. Retrieved July 1, 2016, from http://smallbusiness.house.gov/uploadedfiles/4-22-2015_updatedmemo.pdf

[2] New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity; Majority Have No Policies or Contingency Plans. Retrieved July 1, 2016, from https://staysafeonline.org/about-us/news/new-survey-shows-us-small-business-owners-not-concerned-about-cybersecurity

to push women-owned firms out of the federal marketplace – only months after reaching the 5% goal for the first time[3].

Defense Federal Acquisition Regulation Supplement Clause 252.204-7012

In August 2015, the DOD finalized a Defense Federal Acquisition Regulation (DFAR), requiring companies of all sizes to safeguard Unclassified Controlled Technical Information (UCTI) that resides on their information systems.[4] Controlled technical information is defined as technical data or computer software with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination and is marked in accordance with DOD instructions.

To follow this rule, a federal contractor is required to be compliant with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 – guidelines for "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." The goal is to provide minimum standards to protect government information that finds its way into contractor information systems.

These guidelines have been tailored for private entities including contractors and research institutions. They include 14 "families" of security requirements (commonly known as security controls or security objectives) that must be satisfied. These groupings range from identification and authentication to physical protection.

Contractors that do not implement safeguards for the 14 "families", must submit a written explanation of why the required security control is not applicable, or explain how an alternative control or protective measure is being used to achieve the same level of protection.

Due to the high compliance burden of this new policy, the Defense Department revised the rule in December 2015, to give contractors additional time to implement the security requirements by December 31, 2017. While giving businesses additional time to comply may be helpful, it is clear from speaking with other small contractors many do not have the resources to comply with this rule.

---

[3] SBA: Federal Government Breaks Contracting Record for Women-Owned Small Businesses | The U.S. Small Business Administration | SBA.gov. (2016, March). Retrieved July 1, 2016, from https://www.sba.gov/content/sba-federal-government-breaks-contracting-record-women-owned-small-businesses

[4]Guidance to Stakeholders for Implementing Defense Federal Acquisition Regulation Supplement Clause 252.204-7012 (Safeguarding Unclassified Controlled Technical Information). (2015, August). Retrieved July 1, 2016, from http://www.acq.osd.mil/se/docs/DFARS-guide.pdf

This past February, the SBA office of Advocacy found that the DOD rule grossly underestimated the number of affected small businesses[5]. DOD's estimates only included small business prime contractors, though the rule extends to tens of thousands of small business subcontractors in the federal supply chain.

The Office of Advocacy recommended that the Defense Department collaborate with universities and other organizations to provide low-cost cybersecurity services to small businesses participating in the federal acquisition process or provide a one-time subsidy to small contractors participating in the acquisition process to cover the cost of consultations with third-party vendors. The Office of Advocacy also found that the cost of compliance with this rule will be a significant barrier to small businesses engaging in the federal acquisition process.

While all 14 "families" of security controls may not apply to every company, the standards are clear that information security is not just for information technology contractors like myself. Understanding and managing information security risks can be challenging, especially for companies that are not in the business of cyber security.

National Industrial Security Operating Manual Conforming Change 2

Even more concerning than the recent change to the DFAR is the May 18, 2016 National Industrial Security Program Operating Manual (NISPOM) Conforming Change 2[6], commonly referred to as the "Insider Threat Program." The regulation stems directly from concerns over contractor employees' ability to bypass security safeguards. This regulation requires contractors gather, integrate, and report relevant credible information that may indicate a potential or actual insider threat.

It is especially burdensome for small businesses because it has to be implemented by November 30, 2016 and for the first time, the Defense Department is requiring businesses to appoint a senior level W2 employee to serve as Insider Threat Program Senior Official (ITPSO). The ITPSO must serve in a position within the company that has the authority to provide management, accountability and oversight for implementation of the insider threat program.

For some women-owned businesses, this means they have to hire additional personnel to comply with this requirement. Additionally, in order to adequately report compliance with this regulation, women-owned businesses may have to invest in technology to assist them in detecting, analyzing and reporting on insider threats.

---

[5] Interim Rule, Defense Federal Acquisition Supplement: Network Penetration Reporting and Contracting for Cloud Services | The U.S. Small Business Administration | SBA.gov. (2016, February 29). Retrieved July 05, 2016, from https://www.sba.gov/advocacy/2-29-16-interim-rule-defense-federal-acquisition-supplement-network-penetration-reporting

[6] Defense Security Service Industrial Security Letter ISL 2016-02. (2016, May 21). Retrieved July 1, 2016, from http://www.dss.mil/documents/isp/ISL2016-02.pdf

Cyber Security and the Small Business Community

Lack of technical knowledge is not an excuse for failure to comply with basic cyber security regulations. While it may be difficult for individuals without a technical background to understand the intricacies of these new guidelines, small businesses need to proactively do the following:

- Understand the scope and impact of changes on the business
- Align organizational policies, practices and procedures to comply
- Empower those with the technical expertise necessary to implement the changes
- Provide adequate training to ensure employees are aware of their responsibilities, and
- Hold individuals accountable for compliance

Unless properly managed, information security compliance can be a very costly proposition. Companies that do not have a solid understanding of information technology and information security find themselves reacting to an ever-changing sea of regulatory requirements that will be costly to implement.

While many small businesses are looking to the cloud and its host of services as a way of managing costs, doing so without understanding the security implications can increase the company's security posture to an unacceptable risk level.

New contract guidelines require a small business to rethink an existing product, service, or process, thereby introducing unplanned costs. Management needs to understand the scope of security requirements and ensure that they are incorporated into buying decisions, product and services contracts, service level agreements and human resources processes.

The first step is to get a jumpstart on the new requirements by assessing current information systems and determining changes necessary for compliance with new guidelines. Implementing effective governance processes can help small businesses manage information security risk, increase stakeholder confidence and reduce the costs associated with compliance.

To that end, small businesses could use assistance in determining their cyber security needs. WIPP supports the intent of H.R. 5064, the *Improving Small Business Cyber Security Act of 2016*[7] introduced by Representative Richard Hanna, which was included in this year's defense authorization. The legislation authorizes Small Business Development Centers (SBDC) to support small businesses in developing affordable cyber security plans. However, we would encourage the Committee to consider adding other SBA resource partners, including over 100 Women's Business Centers to do this outreach.

---

[7] H.R. 5064 Improving Small Business Cyber Security Act of 2016. Retrieved July 1, 2016, https://www.congress.gov/bill/114th-congress/house-bill/5064/text?q=%7B%22search%22%3A%5B%22Improving+Small+Business+Cyber+Security+Act+of%22%5D%7D&resultIndex=1

In conclusion, women entrepreneurs consider the federal marketplace a key opportunity to grow their businesses. With more than ten million women business owners nationwide, competition for government opportunities among women innovators and entrepreneurs remains strong. While there is a need to protect federal data, and small businesses need to protect themselves from cyber attacks, the government has gone too far with these new regulations. One size does not fit all. Ensuring that new cyber security requirements are attainable for small businesses is of paramount importance. This Committee has always acted in a bipartisan manner to support women entrepreneurs and we appreciate your examination of this issue, making sure that these requirements achieve the desired results, rather than more red tape.

Thank you for the opportunity to testify and I am happy to answer any questions.