Testimony of Michael MacKay
Cyber Security Subcommittee of the Senate Armed Services Committee
March 26, 2019

Introduction

Chairman Rounds, Ranking Member Manchin, and Members of the Subcommittee, I would like to thank you for inviting me to testify this afternoon. My name is Mike MacKay and I am the Chief Technology Officer of Progeny Systems Corporation.

Progeny Systems is a privately held defense contractor headquartered in Virginia that has just under 500 employees. Progeny Systems is in the category of "small large Government contractor" and is a significant target for cyberattacks, due to both the highly classified nature of our work and the number and types of our contracts. We know that attempts have been made to penetrate our network defenses and we are fully dedicated to the implementation of the Government's recommended policies, procedures, and controls as detailed in the NIST Special Publication 800-171 (NIST).

As the Chief Technology Officer of our company I can tell you that cyber defense is a top corporate priority. It is a priority because of the responsibility we have to our customers, and we fully understand that, as a small company, our very survival is at stake. We are not a large prime contractor that is "too big to fail and too big to punish" and that the first breach could be the last one.

Most importantly, cyber defense is a priority because all of our employees understand as Americans the threat our adversaries pose. Our overriding goal as a company is providing our warfighters with a competitive advantage no matter the battlespace. We cannot let our nation's adversaries steal technology that diminishes this advantage, and we have invested heavily in equipment, tools, and manpower to ensure that the NIST specifications are not only met but exceeded.

One Standard

Thus far, we have been reviewed by only one program office for compliance with NIST's requirements. We do not, however, have only one program office as a customer. We work for dozens of programs who each may have a slightly different interpretation of the NIST's requirements. Smaller companies will find it impossible to be rated favorably if they are pursuing two or more different interpretations of the controls and what is to be considered adequate or complete. As the Committee considers this issue, I would strongly urge you to have one standard interpretation of NIST's requirements. Set the bar high, but set it once and hold everyone accountable to that single standard, so that we are not only spared the additional cost, but also spared the need to adjudicate between differing and potentially conflicting direction.

Importance of Human Factors

We view the NIST requirements as essentially putting locks on your doors and windows and installing a security system. These measures are effective in keeping people out of your house

and letting you know if someone tries to break in. They are useless, however, if you open the door to a stranger who wants to rob you. This where private sector defense contractors need the most help - in the human factors.

We need to raise awareness and to train our personnel to think of good cyber security hygiene as a natural part of their daily work lives. For technology developers who crave connectivity and collaboration, this is a huge paradigm shift. This is especially the case with younger technology developers who, unlike us, grew up online and are more susceptible to Phishing attacks.

The guidance provided to date for training has been to seek out peers and share lessons learned. Although we are doing this, we need to more effectively confronting this threat. The Department of Defense must take a leadership role, and we need evidence based best practices, curriculum, and effective training materials to educate our employees. Cyber defense requires both tools and training to accomplish the mission.

Adapting Cybersecurity Requirements Based on Contractor Size and Ability to Pay

As a smaller company with limited resources, we feel that there is merit to adapting the Cybersecurity requirements based on each contractor's particular situation, size and budget included. However, we must protect the technology according to its importance, and find ways to help that industry partner, small or large, to protect it. Often, the smaller companies, who have limited resources, are also those with significant innovations. We can have the best of both situations if we help those innovators continue to safely pursue their work.

Offer Cybersecurity Expertise and Red-teaming to Contractors

A major tenet of our development community is that "No one has all the answers". Progeny Systems received help from one of our Program Offices, in the form of a two day exercise with industry experts in a "mock audit" of our practices in January of this year, to review our status for 800-171 compliance, and the event was eye-opening and invaluable. A standardized, consistent, and regular consultation with experts and Red Teams would probably be the single most beneficial approach that could be offered by the DoD to its contractors.

Provide "off-the-shelf" architectures and products

We wholeheartedly agree that providing "approved" products to the community by the Government, based on a "best of breed" selection process will be an excellent way to help the community protect themselves, especially if, as in the case of smaller companies, there are resource issues with acquiring or developing the correct controls and protections themselves.

Closing

I want to thank the Subcommittee once again for having the privilege to testify before you today and would be happy to answer any questions that you might have.