

To: Kevin Kimball, Chief of Staff, National Institute for Standards and Technology (NIST), Department of Commerce

From: Scott Nelson, Vice President Outcomes and Strategic Partners, SecureSet Academy

Date: August 2, 2017

Re: NIST Cybersecurity Workforce RFI

**Summary:**

SecureSet Academy (SSA) brings the bootcamp model to cybersecurity education with comprehensive, practical programs for launching your career or upping your tradecraft. We partner with top employers to provide the skilled talent the industry is searching for. We have designed community based cyber security pipelines for transitioning active duty military, career transitioners, IT professionals looking to transition into security, and other foundationally qualified students looking to find a career in cyber security.

Our ([approved](#)) CORE program is your direct path to a cybersecurity career. This 800-hour immersive curriculum includes twelve foundational courses, extensive hands-on skill building, and guided product training (full time; see the evening comparison below).

CORE students graduate with the sought-after knowledge and tradecraft for immediate employment as tier 1+ security engineers, analysts, pen testers and consultants. The evolution from general IT to cybersecurity can take five to 10 years. The CORE does it in as little as 20 weeks.

Our ([approved](#)) HUNT program is your direct path to a cybersecurity career in an Analyst role. This 480-hour immersive curriculum includes eight foundational courses, extensive hands-on skill building and guided product training.

HUNT students graduate with the sought after knowledge and tradecraft for immediate employment as tier 1+ security analysts, threat analysts and hunt analysts. The evolution from general IT to cybersecurity analyst can take three to 7 years. The HUNT program does it in 12 weeks.

The solution to the cyber security professional supply is building community based cyber security pipelines from middle school, high school, through vocational education into multiple channels of employment (military, government, industry) and articulated

into higher education. SecureSet has built these models in all three of its campus locations; with over 34 employers (local, regional and national), military organizations, community based Cyber centers (Florida and Colorado), multiple Universities, High Schools, non-profits and industry associations.

### **Are you involved in cybersecurity workforce education or training?**

- SecureSet is directly involved in developing a robust cyber security talent pipeline for the communities we serve. We are currently operating programs that serve High School students by building a 4-year Information Security/ Cyber Security curriculum. SecureSet is focused on building a robust entry level cyber security program to build tier 1 and 2 Security Analysts, Security Engineers, Cyber Threat Intelligence Analyst, Penetration testers and Security Consultants.
- We have also launch a first of its kind Department of Army Cyber Security Career Skills program to educate transitioning Active Duty personnel into Cyber Security careers. These active duty personnel spend their last 6 months on active duty at SecureSet in the CORE technical 20-week program. The program integrates national level employers who sponsor a Soldier and then place them in a cyber security position in their company.
- Finally, we operate with numerous partners from industry and academia to continue the cyber security pipeline either through placement in cyber security positions in over 34 companies and for those who have not completed a 4-year degree, opportunities through articulation agreements to complete their degree at a 4-year university. The current CORE program will articulate to Norwich University and Colorado State University (Global) for 34 and 33 credit hours toward 5 different bachelor degrees at each University. Our hybrid model will build further articulation agreements with regional public or private Universities as we launch new campuses. 3-6 campuses planned for CY 18 in communities critically short of cyber security professionals.

### **Is there sufficient understanding about workforce categories, roles, knowledge, skills, and abilities?**

- The problem with the industry today is they continue to follow the old model for hiring Cyber Security professionals, especially new entries/ entry level personnel. HR managers are looking for 5-7 years of experience in IT and Security, plus multiple certifications to validate the candidate is qualified. Many Hiring managers and HR directors struggle with what qualified looks like so they maintain hiring practices that cannot fill the void for their critical vacancies and don't discuss ways to improve a broken system. The NICE knowledge, skills and attributes are a good start for

defining the KSAs for government but they have not broken into industry in a large way. With a growing skills, workforce and talent gap, currently projected in the United States to move beyond 350,000 vacancies, a new model for developing entry level personnel is required for the United States to maintain economic and national security superiority.

- SecureSet 's hybrid education model balances theory and application to provide immersive cyber security education across 7 different courses. The model includes an aggressive placement process that builds graduates attractiveness to 34 hiring partners and growing. SecureSet is educating and demonstrating the skills of our graduates, allowing hiring partners to build trust and confidence that graduates will immediately be ready for work. To date, SecureSet has graduated 35 graduates in Denver, with 100% employment of graduates within 120 days of graduation. By December, across three campuses in Denver, Colorado Springs and Tampa; SecureSet projects graduating and additional 85 to 100 graduates by December 2017.

### **What are the most effective domestic cybersecurity education and training programs?**

- The results from the eighth Global Information Security Workforce Study (GISWS) were released earlier this year. The cybersecurity workforce gap is estimated to grow, with the projected shortage reaching 1.8 million professionals by 2022. The rapid evolution of technology and threats further complicate a national crisis in building an effective cyber security workforce.
- The nation is at risk from this severe shortage of cyber Security professionals. One of the main problems is the lack of a robust national cybersecurity workforce pipeline focused on building entry level professionals. The solution may be a hybrid education model that applies vocational, experiential and higher education models.
- Here are a number of them but each serves a specific segment of the cyber security workforce pipeline. The well-known providers for advanced and experienced cyber security professionals include SANS and other certification shops. The problem exists that the pipeline for these professionals is too small and slow to fill the talent gap that continues to explode.

### **SecureSet Hybrid Model:**

One model that is producing promise is the SecureSet model, a hybrid immersive model that integrates multiple pipeline partners to produce cyber security

professionals. Identifying a community based cyber security baseline that focuses on entry level development of cyber security professionals across 2 programs; very technical 20-week CORE program that produces entry level Security Engineers, Security Analysts, Security Consultants and Penetration testers. The program graduates possess the skills to enter the workforce with critical skills to make them successful as Tier 1 or 2 professionals in these careers. The second program is the 12-week HUNT analyst program that produces Tier 1 to 2 Security Analysts, HUNT Analysts, and Threat Intelligence analysts. The success of these programs is already apparent with a 100% placement rate to date (with 120 days of graduation), 100% pass rate of graduates that take CISSP and Security + certifications and opportunities through articulation agreements with high quality Higher Education partners to complete a bachelor degree in a security related degree. The key to this success is the design of both programs that produced comprehensive and technically competent entry security professionals through an immersive mix of Cyber Security theory and vocational like application. Industry input is critical to the development of an effective entry level cyber security education program. SecureSet used intensive and repeat interviews with over 30 companies to identify critical knowledge, skills and abilities (KSA) that each company required. The industry input produced a comprehensive list of KSAs across 7 courses in the CORE program and 7 courses in the HUNT program. These courses include Network and System Security; Applied Cryptology; Governance/Risk and Compliance (GRC); Strategy and Analysis; Cyber Threat Intelligence; Logs and Detection; Hunting and Security Culture.

SecureSet Academy (SSA) is partnering with University of Colorado – Colorado Springs (UCCS) to enhance the Colorado/National Cyber Center (NCC) program in the Cyber Research, Education, Training Center (CRETC) in development of initial NCC Cyber Security applied education and training programs. The intent of this partnership is to build initial operating capacity of NCC CRETC that can better serve individuals interested in pursuing careers in the cybersecurity industry including recent high school graduates, minority and under-served populations, career transitioners and Colorado military population. SecureSet Academy and UCCS will also collaborate on the development of a K-12 Cyber Security program that builds foundational skills in Colorado high schools to allow multiple paths into the Cyber Security workforce. SecureSet Academy is a Colorado Department of Higher Education approved institution that provides proprietary, hands on education on cybersecurity that is designed to produce entry level security analysts, engineers and consultants.

**What are the greatest challenges and opportunities facing the nation's cybersecurity workforce education and training?**

There are numerous problems with the current traditional model for cyber security education and training.

1. Traditional Recruiting /HR model does not work.
2. Higher Education does not have resources or skills to rapid transition to support rapid evolution of cyber security career field.
3. Current educational and training (What we have been doing is not working, we are falling behind and not catching up.

Standard practices of recruiting people with 10 years with systems or network administration then transition into security does not work. 1.8 million vacancies by 2022. Traditional education is not effectively delivering the workforce necessary for the massive demand for these professionals. The reasons include: cost, missing standards (NICE emerging), emerging field (lack of professionals in the field), industry is not involved with development of education programs. Each community needs a new strategy that builds a workforce development pipeline. This would be a hybrid education model that focused on development of technical skills linked with nontechnical soft skills, policy and GRC roles. Hybrid is a public/private model. Includes K.12 programs through High School to build foundational IT and embedded/comprehensive security skills. Develop public/private Cyber Centers that include Industry, government, academia, military and primary education.