iQ4 Corporation & Cybersecurity Workforce Alliance (CWA)[1]
Response to NIST RFI 02 August 2017 - Document Citation 82 FR 32172
Comments on Growing, Sustaining the Nation's Cybersecurity Workforce

Introduction - Solving Cybersecurity Workforce Growth and Sustainability Issues

Nowhere is the workforce skills gap more pronounced than in cybersecurity. A June 2017 report from Cybersecurity Ventures estimates 3.5 million unfilled cyber jobs within the next 4 years, coincidentally the typical time period it takes to fulfill college undergraduate degree requirements. Or is it a coincidence

Prominent investors, Richard Craig Baum and Jim Rogers opined in a July 10, 2017 commentary for "Fortune" that continued failure to provide a skills-ready workforce "will likely burst with the force of all previous catastrophes combined—a shock wave so sudden, so large, that it gathers the full force of the savings and loan, insurance, energy, tech, and mortgage crashes, creating a blockbuster-level perfect storm." Other commentators are also hitting the economic panic button and predicting a Depression-level fall out from private sector skills gaps. Perhaps this is why organizations like the respected Lumina Foundation have a growing interest in Contextual Education.

With the growing gap and a dwindling pipeline to fill it, the invisible hands of market supply and demand are tied. A new model is needed which aligns academia and industry and connects students directly with professionals to provide contextual, practical and sustainable pathways to pursue their career dreams. A systematic and scalable program is needed that solves the challenges of student (and re-learner's) employability, retention and mobility, which is critical to our nation's economic security.

iQ4 pioneered the technology which enables private sector and higher education partnerships to solve the gaping - and growing - cybersecurity workforce skills shortage. We have developed a Cybersecurity Workforce Alliance (CWA); commencing in private sector investment banks (member banks of the New York Federal Reserve), the bank regulatory community (The NY Fed), their industry association (SIFMA - the Securities Industry and Financial Markets Association), and the local city and state universities in New York (CUNY, SUNY Albany and Saint Rose) to build a successful scalable workforce engagement model, that facilitates how higher education can align virtually with industry, particularly in cybersecurity. The CWA mission is to accelerate the readiness of cybersecurity entry-level candidates - and to bridge the gap between graduating with a degree and being "workforce ready" for a career - by learning from industry first.

Since its inception in January 2015, the CWA has become a national movement with over six hundred executives. Within Education, the program alerts students to the great careers and job roles available in Cybersecurity to inspire them into an accelerated contextually based learning courses (Awareness: 99% of the Alumni were not aware of Cyber careers before the course). Within Enterprise/Employers, the program maps the specific skills students and learners need for mobility or up-skilling to improve and advance their careers. The model creates predictive career pathways for employees, while ensuring a "load balance" of resources needed by industry players to maximize productivity and employee retention.

As an apprentice/mentor system, the CWA has begun to revolutionize higher education by being grounded in a proficiency model charged with technical, academic learning, combined with professional skill development and critical thinking objectives. The CWA curriculum is built around the NIST Cybersecurity Critical Infrastructure Framework, which supports the way that organizations meet cybersecurity threats and obligations. Moreover, the 600 CWA enterprise members, representing major financial institutions, consulting firms, and Fortune 100

[1] iQ4 Corp is the CWA technology Platform for Workforce M.I., Skills Development and Career Pathways.

companies, have enhanced our curriculum by developing Essential skills components. These components include team based problem solving; oral and written communication; team-based collaboration; advocacy and leadership. As a result, our students develop the ability to be productive cyber professionals immediately; cutting 3-6 months out of the hiring, onboarding and development process, with a significant return on investment for the hiring organization.

In summary, the CWA has a platform that delivers profound—and sustainable results. We welcome the opportunity to extend our private/public partnership to those that can help scale our solution to secure the national interest of our nation's economic security.

Q1: What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

No holistic or comprehensive metrics and data currently exist in the marketplace for cybersecurity education, training and workforce development. Standards and protocols do exist, such as the current NCWF Framework and NICE Taxonomies ('Cyber Standards'), for companies and organizations to detect, isolate, and remediate cyber intrusions. Nevertheless, these Cyber Standards are not directed to address the development and retention of core human assets through awareness of careers, education, training and workforce development.

What we have developed is a specifically directed, tailored, scalable and sustainable approach that aligns the education and training needs with industry for the full eco-system of cyber skills sets. The CWA has been able to develop a technology, system and curriculum which scales and accelerates cyber skills development by connecting students with industry through real world case studies. It is now possible to collect robust data and build meaningful metrics around assessments, including initial proficiencies and progression (including student self-assessment and, team peer assessments at the beginning, middle and end of their course to inspire them to progress toward a cyber career) and Mentor's applied knowledge assessments of students on a weekly basis that show progression, development and the absorption of knowledge throughout the course. Outcomes may then be measured as well, including determining how many students get internships and jobs in which sectors, and measuring entry level pay bandwidth. These metrics are available:

- How many students enter each CWA course, and in aggregate, which state, schools and faculties they are from; initial awareness of Cyber as a career before the course (currently only 1%);
- The level and extent of any incoming form of employment or internship experience prior to the course (currently only 5%);
- How many are still in college now, but have a cyber-related internship (currently 61%),
- How many have graduated and secured jobs/internships in Cyber roles (currently 33%),
- And, real time data as to student engagement with the program, including activity on the platform and course (currently avg 9 posts/student and avg 93 words/post), who has initiated critical-thinking discussions and how many interactions with the discussion thread from all teams in the semester.

Diversity metrics can be captured and assessed as well. Many of the CWA alumni are female, minorities, veterans and are from diverse backgrounds. Plus many of our students are the first college students from their families. We are leveling the playing field. Dashboards and data can be shared with NIST/NICE; e.g. metrics on throughput and outcomes to be compared with the national and location demand gaps and/or the job availability e.g. as in the NIST CyberSeek data base.

The CWA Co-Curricular/Contextual approach is about extending the workplace into the classroom and taking internships, co-ops, capstones and apprenticeships to a new level of productivity. This is a highly scalable and integrated mentor/student team model where, expertise, capacity (to augment academia), applied knowledge and skills can be measured. Importantly, students now have exposure to real-world experience that enhances their academic learning and makes them more attractive to hire. The CWA has, for the first time, produced Cyber Standards based Co-Curricular/Contextual transcripts recognized by the National Student Clearinghouse (NSC). The CWA and NSC were awarded the 2016 First Prize for Best Practice at PESC (Postsecondary Education Standards Council) Spring Summit for **"Extending the Capacity of Higher Education to Scale The Output of Verified Workforce Ready Graduates**". These Co-Curricular/Contextual Transcripts empower student mobility and workforce skills measured performance throughout lifetime learning. This is captured on the iQ4 Platform in a digital "Skills Passport" showcase, throughout their career. The data is validated for academic and contextual learning. The NSC has 21 million current college students and 340 million college graduate records in its database, so employees, employers and education can rapidly and effectively benefit from this integration, and CWA can supply the metrics generated to multiple stakeholders: government, education, employers, and industry associations.

Q. 2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

While the Private sector has a reasonably well developed understanding of workforce categories, specialty areas, work roles and the attendant knowledge/skills and abilities required for Job Families, this understanding has been either siloed within organizations or limited to an industry or organization's shared knowledge. However, this information has not been accessible or utilized by institutions in higher education. Into this gap, the CWA has driven the adoption of the NCWF into both the private and higher education sectors, with CWA member firms and their employees leading by example. For example, in conjunction with a leading Global Financial Institution, the CWA has, for the first time, systemized the NCWF approach by automating the 4-tier NICE taxonomy and integrated it with their internal taxonomies to define Job Families/Roles across Cybersecurity, Risk and IT. iQ4/CWA has also added a 5th dimension called "Context", which is particularly valuable when (say) adding a KSA for the type of technology/tooling that is required in that role/location/firm. In this way, increasing and positive exposure is created for enterprise organizations to learn about the NICE Taxonomy. They are learning to appreciate its value; understand how to implement it; realize how mature it is and recognize that the NICE Taxonomy underpins the NIST Framework.

The key has been standardization on a technology backbone. Through the CWA approach, both a software platform and curricula have been developed, so that the program can scale rapidly and nationally. Each college or university that adopts the specific modules gains insight, transparency, and definition of the skill sets and roles valued by industry - because iQ4/CWA makes this available as Open Source on the Platform. With that knowledge, course-work directly reflects and aligns with Industry's needs and the Nation is better protected by scaling more people into cyber to close the acute hiring gap. All the roles in our course are based on real world case studies. The technology platform allows "virtual" enablement of the workplace environment and permits active/scalable deployment of mentors to participate within the classroom. Industry mentors provide capacity and expertise to the educational institutions, without adding to the institution's payroll. Students contribute an average of 5 hours per week to the 3-credit, 14-week semester course. CWA mentors willingly volunteer 1-1.5 hours per week to obtain insights into potential new hires, while observing 25 plus students in a class.

Moreover, the CWA course is not just focused on the technology aspects of cyber, but also risk, governance, legal/regulatory and financial aspects. Our course is scalable and adaptable to other contextual learning opportunities in different industries.

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training and are those policies regularly and consistently enforced?

Most enterprises have awareness training programs, but very few have effective training and education programs. Both Academia and Industry have retained iQ4 and utilized its CWA platform. In the case of industry, it has been deployed to develop and implement robust policies, audit trails and assessments for workforce *c*ompetency and skills gaps and professional education. In the case of academia, it is used to develop experiential and accredited curricula to train students to enter the workforce aware of governmental standards such as NCWF, NIST and NICE as well as relevant organizational standards for continuing career and professional development.

Specifically, within organizations, employers benefit from the automated taxonomy to identify training needs: enterprises can profile the skills of their entire workforce. An individual's profile-to-KSA taxonomy mapping is core to the solution. The individual can be assessed for proficiency against each KSA. Then, iQ4's technology can identify and offer learning and career pathway opportunities for the individual. The platform can also be used for Cyber awareness training, with digital badges and certificates certifying the currency, level, and renewal information for cyber awareness training by individual. The NSC can also verify educational and co-curricular/contextual transcripts. Dashboards and analytics show C-suite, managers and regulators real-time skill level and compliance with training policies, and where skills or gaps exist down to the weakest KSA by region, location, business unit or individual. Management can then plug the skills gap with learning, development and/or employee and contractor mobility, utilizing the iQ4 Platform "Skills to Role" matching engine. Management will use Role Profiles to define "Target State," and use Skills Passport assessments to define "Current State". The outcome is the ability to automatically recommend specific LMS courses, as they are mapped to NCWF competencies to improve skills and productivity. In turn, employees are now empowered to map their current skills with opportunities that create pathways for their career based on the skills framework. As a result, employee mobility results in high gains in work productivity and retaining the workforce over time (e.g. increase employee retention by 2-3% saving millions of dollars in lost productivity and costs, CWA member reported replacement cost at $121K/ea.)

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (e.g., energy vs financial sectors)?

Employers need to convey the appropriate and relevant standards and frameworks, such as NIST, NICE and the like, so that they can value the experience and knowledge of their incoming and/or existing employees. Specifically, the core attributes that employers need/value from entry-level candidates include **knowledge of the NCWF Framework (the workforce skills needed to support NIST), how it operates *plus* critical thinking, team based experience, ability to research and describe outcomes, communication skills, self-confidence, etc.** CWA member expectations on outcomes are realistic because they are able to directly modify and design curricula to tailor to their exact needs. Thus, CWA curriculum is constantly being enhanced. Industry designed curricula creates the sustainable model that scales and accelerates student awareness and workforce readiness. By allowing Industry to design curricula, the college/university student workforce is prepared faster and more effectively, when using the NIST Framework and NICE taxonomy. This allows the workforce to become more attractive to hire, and to bring almost immediate value to public/private sectors by improving an organization's Cybersecurity resilience and capabilities. In addition, organizations can better identify their talent, motivate them with career pathways and lifelong learning, create project teams quicker, load balance projects with the right resources at the right time. The ability to implement best practices around people, governance and processes to maintain the framework provides efficiency improvements, including data-based targeting to save millions of dollars through increased productivity and improving employee retention.

The CWA has found that the types of Cyber knowledge within organizations vary by role. Like real-world workforces, the CWA curriculum is applicable across all academic majors/disciplines with the initial coursework being built around the "Threat Within", in the context of Financial Services. Nevertheless, CWA alums obtain cyber-related jobs in all industry sectors, not just financial services. This proves that employers place the highest values on workforce readiness skills (not degrees) aided by a 3.5 months of Cybersecurity experience from a team and role based virtual-internship, so employers do not seek different entry-level KSA requirements by sector/industry. Indeed, because CWA cross-sector members contribute to the NCWF Taxonomy, the KSAs employers need or value as they build their cybersecurity workforce are those in the "current" Taxonomy, so employer expectations from NICE are being met. Using the same taxonomy and skills for the existing workforce and student pipeline bridges education to industry. The CWA's contributors ensure the NCWF taxonomy can sustainably evolve with market dynamics. Cross-sector input and automation means the flexibility of compiling a Role around KSAs, as "Required" or "Assets", is enabling common understanding and transportability of definitions for cross-sector workforce specialties and mobility.

The challenges however go beyond cyber. We have a shortfall of STEM graduates as well. These shortages will impact certainly our economic growth and national security, if they are not addressed now.

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

*Th*e CWA believes that our model produces the most effective cybersecurity education, training, and workforce development program being conducted in the U.S. today for industry based "contextual learning." It is effective because:

1. It is focused on college students, which allows the program to easily scale through a national reach; it levels the playing field, and has delivered a sustainable pool of a next-generation workers.
2. The iQ4 Enterprise model (on the same platform) overcomes many of the challenges facing the Nation, employers, and workers, because it helps employers identify area of workforce risk, while facilitating opportunities and solutions for career pathways to plug gaps with upskilling, progression and mobility.
3. The automated NICE/NCWF taxonomy drives data analytics for employers to describe to Education what they need in terms of KSAs (Learning Outcomes) to fill their changing/priority hiring needs.
4. Speed: new modules can be developed and implemented within weeks, rather than waiting for two years to get curriculum implemented and another 2-4 years to benefit from any degree output.
5. The CWA program is based on real-world experiential learning derived from Epic [Business} Challenges/Projects packed into 3-credit course. On the job training while students are in the classroom.
6. The structured curriculums take students through the NIST infrastructure to complete a team and role based contextual problem solving cycle in Cyber. This develops knowledge and experience on the topic through critical thinking, research/analysis/reporting, and communication - the Essential skills, as opposed to the academic approach of "learn and show me how much and how eloquently you can recall".
7. Mentors measure progression and performance by assessing individuals and teams on a weekly basis, using a four tier rubric agreed between industry and education (1) Novice (2) Baseline - Theoretical Knowledge (3) Proficient - Practical Application and Experience (4) Experienced - Role Model.
8. The 3-months virtual mentorships counts as if it were a physical internship. Moreover, CWA members state that it is often more effective because they do not have to invest so much time in shadowing interns and for just 1.5 hours a week, they can mentor a class of 24 interns instead of just one intern on-premise.
9. The skills developed in the course are mapped to the Job Role the intern is playing (InfoSec, Intel Analyst etc).

10. Liberal arts students get exposed to business and cyber operations with some exposure to Frameworks, tools and technology, which Cyber team members may have to use soon after entering employment.
11. The CWA students are engaged thoroughly during the virtual internship: students average one post/week with an average of 93 words/post with guidance and response from mentors.

Industry ultimately needs to train and invest in a new higher education ecosystem. The CWA can provide the platform and enabling technology to deliver a scalable solution.

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers (access to internships, experience and skilling in terms of cybersecurity education, training, and workforce development?

The greatest student workforce challenges include:

- Capacity/Expertise - Lack of Cyber knowledge among faculty and career awareness amongst students regarding career opportunities in cyber;
- Sustainability - The funding necessary to endow contextual learning programs, specifically to address acute workforce needs and skills like cyber;
- Scale - The expense and limitations on physical internships, from a ratio of 1 academic monitor to 2-3 students, to 2-3 CWA/Industry mentors to 20-30 students through a virtual internship.

The scalable, virtual nature of the CWA program overcomes these limitations. Virtual-mentorships allow for every student to get mentored by one or more industry experts. For example, one of our member colleges had one faculty member facilitating 19 teams totaling 106 students during the Spring semester 2017, which ended in a measureable success. The Acting Dean stated: If these internships were physical, between 10-15 faculty would be engaged in monitoring and administering the same number of students. Also, potentially, each mentor's firm would take on only one Intern rather than mentor 24 in a class (3 teams of 8) at a time.

An additional challenge is aligning incentives for the private sector from the public sector, to make significant investments in programs like the CWA. The CWA believes that in order to ensure that the U.S. has workforce ready, entry level, cyber professionals, we must create specific tax incentives for enterprises to endow programs like the CWA. These tax incentives are necessary to initiate investments in programs that can remedy the acute shortage of entry level cyber professionals, and can be earmarked for funding programs geared to veterans, community colleges, colleges in impoverished cities and states, etc.

The CWA has proven that it can generate workforce ready, entry level cyber professionals based on our results at CUNY and SUNY Albany since 2015. We believe that funding a team of ten college students for one semester in our program for $25,000 will generate a minimum return on that investment of a 10x, based on the most conservative assumptions. This return is based on the following assumptions:

- There are no recruiting costs to hire any of these students;
- Based on the semester long internship, *the post hire training time frame is cut by 3-6 months*
- New hire retention is higher because these new hires have made an informed career decision to enter cyber and have built a loyalty toward the hiring mentors; and
- These new hires will be productive from day-one either generating revenue and/or saving expenses related to their cyber roles.

If enterprises are incented through enlightened public policies *and see a proven attractive return on investment*, then we will achieve the desired result of enterprises endowing such initiatives as the CWA. This is a danger that enterprises are becoming desensitized to cyber threats--nobody is secure, so why bother. According to the 2017

State of Cybersecurity Metrics Report, more than half of respondents to a survey scored an D or F grade, when evaluating their efforts to measure their cyber investments and performance against best practices.

The greatest opportunity for next generation and enterprise workforce is for CWA cohorts to be created around colleges/universities and community colleges to supply entry-level graduates to employers. The CWA course is scalable and can be set-up in 6-12 weeks. The CWA model can be applied nearly universally, and cross sector collaboration by members, guided by CWA's senior industry Advisory Council, to ensure sustainability, as the members are self-motivated to modify the curricula, while recruiting volunteer mentors to grow the program.

We simply need to expand collaborations between higher education and industry. The CWA has the platform and expertise to facilitate this collaboration.

7. How will advances in technology (e.g., artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?

Advances in technology such as artificial intelligence, IoT, autonomous vehicles, etc. will serve to widen the skills gap between workforce-ready students and industry. This skills gap is growing rapidly (see cybersecurity increase 2017 to 2021), and in order to combat this, iQ4's objective is to create a transparent infrastructure that extends the workplace into the classroom. "Contextual Learning" is a model that provides a transparent connection between the needs of the workforce and higher education, as industry is able to adapt and respond to changes in cyber in real-time, and communicate its changing needs to students and higher education directly. "Contextual Learning" serves as the framework to facilitate knowledge sharing, and complements "Academic Learning," driven by education and industry together, with tools, models and content that generate measured outcomes. CWA courses are being adjusted as required to include technology threads and training, where appropriate, to fully embrace KSAs in People, Process and Technology.

8. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken: i. At the Federal level? ii. At the state or local level, including school systems? iii. By the private sector, including employers? iv. By education and training providers? v. By technology providers?

The CWA believes that we would generate a minimum of 100,000 workforce ready, entry-level cyber professionals within four years, if we were given the opportunity to scale our program nationally.

The CWA has a proven model that is producing workforce ready graduates for cyber, entry level positions. We have and are engaged with higher education decision makers nationwide, who are very interested in our program and results, and wish to bring the CWA to their campus. We have enterprises that provide volunteers to mentor our students weekly during the semester and now are hiring these students. What is missing however, is a comprehensive program to endow a national solution to a national program, funded by those who would benefit from creating workforce ready, cyber entry-level positions: the private sector.

$200ml is a fraction of the estimated $600 billion spent on corporate training and development. $25ml per semester would create an additional pool of 12,500 entry level cyber professionals every fall or spring. The demands for entry-level cyber professionals are growing significantly, as the threats grow and new technologies gain commercial acceptance like the Internet of Things, Artificial Intelligence, self-driving vehicles, etc.

Our program is solving the entry-level cyber challenge:

- our student alumni are pursuing careers in cyber;
- the return on investment for funding our program is at least a 10x based on conservative assumptions;
- higher education and students have embraced this contextual learning solution, to expose a cross section of undergraduates to careers in cyber; and
- enterprises have their CIOs, CISOs and IT executives, volunteer an hour or more of their time weekly, to mentor the students.

In Enterprise, the adoption of the iQ4 Workforce M.I., Skills Development and Career Mobility Platform will complement and augment any workforce development investment that flows through from NIST/NICE NCWF Framework and higher education-to-employer people supply chain.

However, in Higher Education, we are solving the problem on a very small scale. We are seeking the funding through creative, innovative public policy, to incent the private sector to work with the CWA and our higher education partners to fund the CWA at campuses across the country. We believe that an investment of $25ml per semester over four years will generate 100,000 workforce ready, cyber professionals that will generate a cumulative $2 billion return. Moreover, investments like this one will keep these jobs in the U.S. for these graduates, rather than being outsourced elsewhere.

This is an opportunity disguised as a crisis for the Nation. Addressing this workforce challenge now is vital to our national and economic security, as well as our maintaining our technology innovation leadership, worldwide.

The CWA is not an abstract theory, but a working and proven model, that produces results and fulfills its mission. Students, higher education and industry are aligned on our program and mission. We simply need the incentives for enterprises to invest in this worthwhile endeavor, to address not only a workforce issue today, but a national security issue tomorrow.

This document was prepared and submitted on behalf of the iQ4 and the CWA by Frank Cicio.