# Response from OntoPilot LLC
# to NICE RFI
# August 2, 2017

## Growing and Sustaining the Nation's Cybersecurity Workforce

2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?
No. Some attention is given to training people for preventing intrusions, identifying known vulnerabilities in existing code and updating operational systems with remedies to known problems. However, practically Zero attention is paid to diagnosing errors that occur in operational systems and practically Zero attention to finding the faults not found in Test and Evaluation before software containing latent bugs is deployed.

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce?
Employers need a way to assess the system-wide integrity of their deployed software (the real system as contrasted to the envisioned, intended, modeled, simulated versions).
Are employer expectations realistic? No.
Why or why not? Naïvety about the system principles of dynamic and integrity limits and how to assess and assure sufficiency of both. Presumption of adequacy of V&V and T&E even though data clearly shows that latent bugs are deployed.
Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? Realistic expectations are not consistent with the workforce or pipeline. Methods and tools for assessing system-wide integrity of software are not taught in universities or corporate training programs.
How do these types of knowledge and skills vary by role, industry, and sector, (*e.g.,* energy vs financial sectors)? Although some variation occurs by role, industry, sector and software languages, the fundamentals are common.

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? No known programs prepare First Responders to immediately

assess the cause of user-encountered errors in deployed systems. Such programs could be effective if they introduced the right kinds of technology, analysis methods and tools?
What are the goals for these programs and how are they successful in reaching their goals? TBD.
Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs? Ready to demonstrate commercialization of Software Integrity Assessment (SIA).

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development? Adoption of Zero-fault ethos for all software.

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? AI provides the potential to make humans in charge again. The Internet of Things will vastly expand the potential risks of faulty software.
How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)? Initial indications are that a 13-26 week course prepares one Software Integrity Assessment practitioner to do the work of five software maintenance persons.

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?
Implement SIA personnel selection and training.
ii. At the state or local level, including school systems?
Implement SIA personnel selection and training.
iii. By the private sector, including employers?
Implement SIA personnel selection and training.
iv. By education and training providers?
Implement SIA personnel selection and training.
v. By technology providers?
Implement SIA automation aids.

We are from Ontopilot LLC, an Arizona-based research and development organization that has spent most of the past decade developing new methods and tools, based on predicate logic, to assure the integrity of software and systems.

Most efforts in cybersecurity are devoted to detecting intrusions and either thwarting them or mitigating their consequences.  We at Ontopilot believe that a fundamental enabler of cyber-intrusions — faulty software — is not being adequately addressed, particularly for already-existing software in both source and object code forms.

Most malware exploits faults in the target software. Removing software faults would make it far more difficult for malware to penetrate system. While the quality of new enterprise software is slowly improving, thanks to a modern emphasis on software quality, a large body of legacy software remains vulnerable. Much of this legacy software is continually maintained and periodically updated, risking the introduction of new faults.

Software maintenance consumes over half the life-cycle costs of software. The maintenance process, however, is generally not supported by methods and tools adequate to quickly find and repair faults or to ensure that changes to software, either through fault repair or feature enhancement, avoid the introduction of new vulnerabilities.  New methods and tools are entering the marketplace, but it will require a concerted effort to bring existing maintenance personnel and new entrants to the maintenance field up to speed on the new technologies.

We are involved in cybersecurity workforce education and training. We have developed training material for Software Integrity Assurance, and we are working with a licensor of our method and tools to develop a training program for the tens of thousands that will be needed to populate this new and necessary field. We anticipate collaborating with colleges, community colleges, Veterans organizations, and high schools in this venture.

Jack Ring
Byron Davies, Ph.D.
OntoPilot LLC
http://ontopilot.com