Circadence responses to NIST RFI on Cybersecurity workforce education or training

Prepared by: Laura Lee, laura.lee@circadence.com, 858-663-4555

General Information

1. Are you involved in cybersecurity workforce education or training (e.g., curriculum-based programs)?

Circadence Corporation is a small business that develops a set of software programs to include the Project Ares cybersecurity next generation training platform. Project Ares provides a customizable workforce development capability inside of a game engine. It incorporates the NICE cybersecurity work role tasks and skills. This platform is used by academic institutions at the high school and university level, commercial companies, government and military cyber mission forces in the US and abroad. Our employees are experts in cybersecurity training and assessment and build scenarios for individual and team training. We create virtual environments with commercial and government cyber tools and adversary malware for players to learn and test in a safe manner. We incorporate Machine Learning to provide a computerized advisor and an assessment umpire that assists their human counterparts.

Growing and Sustaining the Nation's Cybersecurity Workforce

1. 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?

Our Cybersecurity Training and Assessment platform provides numerous activities for players and instructors/trainers to include technical mini-games on key cyber concepts, environments where individuals learn and test on technical tasks, and full mission scenarios where an individual/team is provided with a real-world problem with stated objectives.

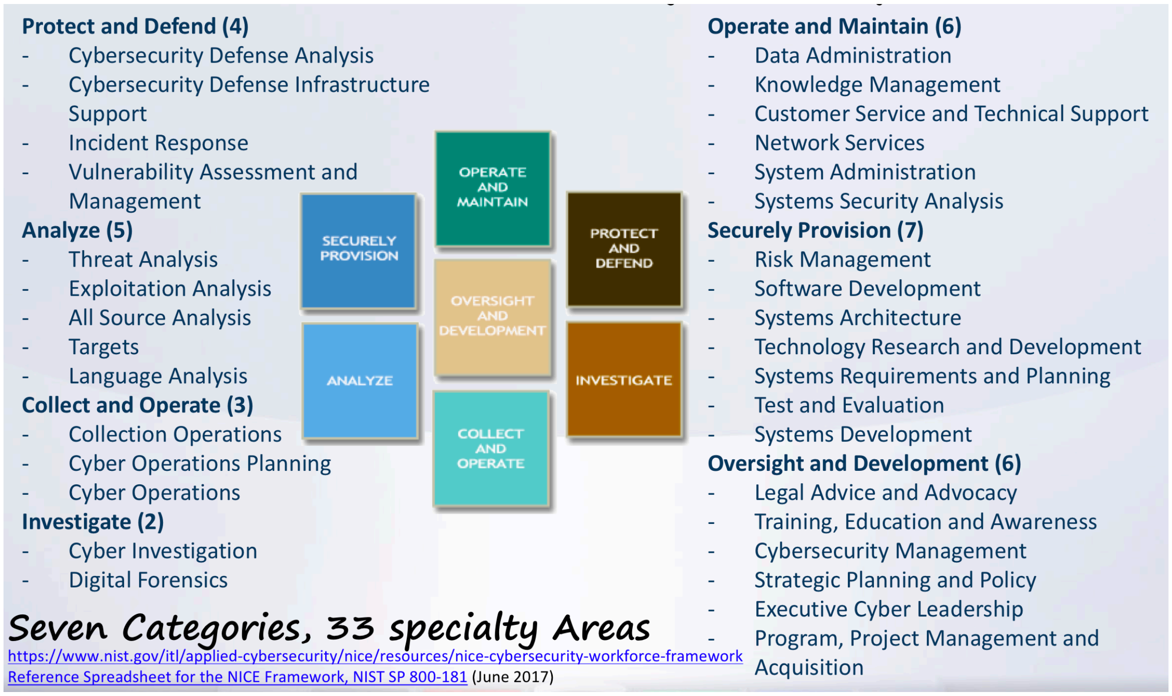
For metrics, we track student tasks completed in a time period, whether or not academic hints were used, trainer comments, player lessons learned and skills/badges earned. We rely heavily on the tasks provided in the NICE Cybersecurity Workforce Framework (NCWF) as a basis of our objectives. When students perform an activity, they earn skill points that are earned when the Artificial Intelligence Umpire detects a correct result.

At the end of a mission, players are given an assessment that is a "record and replay" of their activities. They can see what they accomplished when, the commands they (or their team mates used), chat messages among the team or with the advisor, trainer comments etc. This is stored as a permanent record of a player's performance and is available to the organization as a training report.

Desired improvements in the process of supporting metrics include: creating tasks, conditions and standards instead of just tasks in NCWF and research on data to support skill points. This later aspect deals with the relative difficulty of the task (e.g., task difficulty in a range of 1-10) and how perishable the skill is (e.g., how often should a cybersecurity professional certify that they can accomplish the tasks).

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

Although NCWF is a good first step at the tasks and skills needed across cybersecurity in general, we believe it does not adequately define roles to support cybersecurity workforce development. The seven categories, shown in Figure 1, represent the broad domain of cyber and encompass 33 specialty areas and 52 work roles. Organizations (and personnel) must determine which work roles are needed to match real-world job openings and scenarios. The ultimate challenge in workforce development is not in the adequacy of individual work roles, but rather in the completeness of the set of work roles as applied to a given scenario that the organization or business expects to face. *Only by considering a full set of work roles in a scenario can the gaps in a cyber defense strategy be seen.* To address this challenge, the Circadence work role development approach starts with a scenario for a mission area.



Protect and Defend (4)
- Cybersecurity Defense Analysis
- Cybersecurity Defense Infrastructure Support
- Incident Response
- Vulnerability Assessment and Management

Analyze (5)
- Threat Analysis
- Exploitation Analysis
- All Source Analysis
- Targets
- Language Analysis

Collect and Operate (3)
- Collection Operations
- Cyber Operations Planning
- Cyber Operations

Investigate (2)
- Cyber Investigation
- Digital Forensics

Operate and Maintain (6)
- Data Administration
- Knowledge Management
- Customer Service and Technical Support
- Network Services
- System Administration
- Systems Security Analysis

Securely Provision (7)
- Risk Management
- Software Development
- Systems Architecture
- Technology Research and Development
- Systems Requirements and Planning
- Test and Evaluation
- Systems Development

Oversight and Development (6)
- Legal Advice and Advocacy
- Training, Education and Awareness
- Cybersecurity Management
- Strategic Planning and Policy
- Executive Cyber Leadership
- Program, Project Management and Acquisition

Seven Categories, 33 specialty Areas

https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
Reference Spreadsheet for the NICE Framework, NIST SP 800-181 (June 2017)

Fig. 1. Current NCWF Categories and Speciality Ares in Cybersecurity are helpful in tracking skills but not in defining work roles for workforce development

For example, to use the NCWF to build a Cyber Defense Team for an organization that can support all the tasks outlined in the NIST Cybersecurity Framework (NIST CSF), we need to include the work roles from the NCWF Protect and Defend category, plus the All-Source Analyst and Exploitation Analyst from the Analyze category, the Cyber Defense Forensics Analyst from Investigate, the Network Operations Specialist from the Operate and Maintain category and the Information Systems Security Developer from the Securely Provision category. Using the NCWF tasks to complete a Cyber Defense Team theoretically results in gathering the 9 work roles across the five categories.

It would be more helpful to start to define a Cyber Defense Team construct that covers the NIST Cybersecurity Framework of Identify-Protect-Detect-Respond-Recover so that all necessary tasks are covered without gaps. We believe that the 52 work roles could be better grouped and refined to support four major use cases for a Cyber Defense Team, Cybersecurity IT Team, Cyber Executive Leadership Team and Cyber Offensive Team (for penetration testing or red team exercises). Each of these four uses cases could then have a set of TEAM work roles that constitute best practices.

For the Cyber Defense Team example, we distilled the information from NCWF for the 9 work roles, their tasks and KSAs (eliminating overlap in some instances) and created a simplified approach to a Cyber Defense Team that can scale to vary large problem sets and organizations. The result is five team positions for Harden, Monitor, Pursue, Coordinate (lead/Intel) that collectively are able to perform 207 tasks representing 112 skills (covering the NIST CSF). We grouped the skills into these positions to insure it was simple, straightforward and resulted in no gaps (little overlap).

The *Harden* position focuses primarily on understanding the risk to the mission and identifying ways to better protect it. Harden looks at the existing security posture, configurations, and possible ways that an adversary might have entered the network. This team member(s) also plays a significant part in mitigating (and preventing reinfection from) the threat when found.

The *Monitor* position gathers all relevant data across the enterprise and creates automated alerts when new accounts are created, policies change, or key host/network intrusion detection systems find anomalous behavior. The challenge with monitoring is automating the processes and tuning the sensors in order to minimize false positives and quickly passing the event to the appropriate staff when necessary. The Monitor team member(s) also has a part in mitigating (and preventing reinfection from) the threat when found.

The *Pursue* position assumes that the adversary is already on the network. They start by performing a vulnerability assessment and use a risk management approach to hunt adversaries by digging deep into known adversary hiding spots using indicators in common covert channels. A team member in the Pursue position is the lead on evaluating system integrity and must be very skilled in adversary tactics. This position is frequently staffed by personnel who previously worked in offensive operations where exploit development and reverse engineering are core skills.

Meanwhile, the *Coordinate* position (which includes both the Team Lead and Cyber Threat Intelligence skill set) works seamlessly to manage priorities internally, as well as communicate externally with senior leadership and law enforcement. Each task in the NIST CSF is clearly aligned to a role ensuring that there are no gaps. The team positions, communication strategy and alignment to the NIST CSF is illustrated in Figure 2.

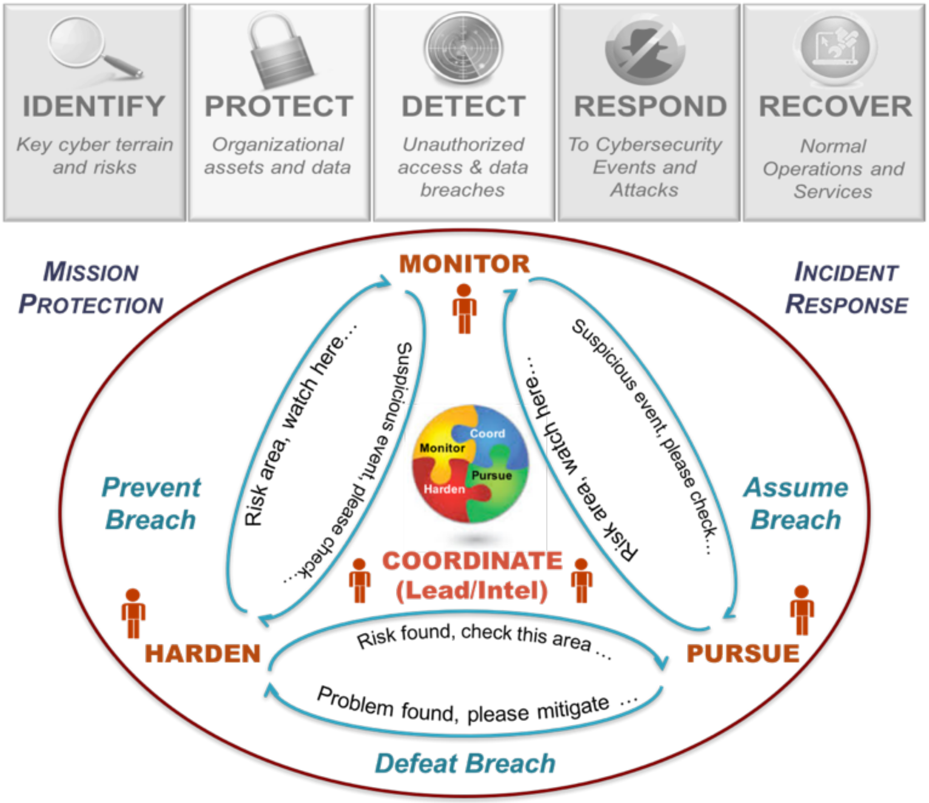

IDENTIFY
Key cyber terrain and risks
PROTECT
Organizational assets and data
DETECT
Unauthorized access & data breaches
RESPOND
To Cybersecurity Events and Attacks
RECOVER
Normal Operations and Services
MISSION PROTECTION
INCIDENT RESPONSE
MONITOR
Risk area, watch here…
Suspicious event, please check…
Suspicious event, please check…
Risk area, watch here…
Coord
Monitor
Pursue
Harden
Prevent Breach
Assume Breach
COORDINATE (Lead/Intel)
HARDEN
PURSUE
Risk found, check this area …
Problem found, please mitigate …
Defeat Breach

Fig. 2. The five recommended team positions for a Cyber Defense Team and their strategy for communications.

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

Yes. Because we are in the business of building capabilities to train and assess the cybersecurity work force, our staff routinely are researching the latest in cyber threat intelligence and building missions to test each other. Organizations face unique challenges when assessing, training, certifying, and measuring the readiness of cybersecurity individuals and teams. As previously discussed, there is a great deal of confusion over the curriculum requirements alone for each individual in cyber. In addition, the challenges of cyber workforce development must be addressed by including several features in the approach:

- Hands-on, safe environment for cyber studies;
- Highly adaptable to handle new concepts, threats, tools, techniques, tactics and procedures;
- Realistic synthetic user behavior within which cyber events will hide/mask;
- Experiential methods that support Gen-X, Millennials and Gen-Z learning styles;
- Objective metrics to evaluate performance against a standard;
- Repeatability in scenarios to try multiple approaches and measure differences in results; and
- Instructional support for the training staff (training material, training/assessment records, realistic environment, progressing management from individuals to teams, and breadth in level of difficulty).

Using Project Ares, our staff can access a media center to review references, watch videos on concepts, or play technical mini-games that reinforce knowledge of ports/protocols/services, adversary tactics, decimal/binary/hex conversion, Internet Protocol (IP) address sub-netting, and other fundamental skills that require frequent use for knowledge retention. Players can participate in mock missions or scenarios that present realistic problems that they need to solve. Users can invite other players online to their team or tackle it alone, but they must possess the problem solving and core cyber skills necessary to complete the mission. The in-game Advisor and Umpire uses machine learning techniques to assist players and give them a final assessment and score.

Through the use of a flexible and customizable framework like Project Ares, organizations can develop their own cybersecurity workforce roles and assess their true readiness to tackle current cyber threats. This approach leverages the expertise of highly skilled cybersecurity professionals by enabling them to mentor entry-level staff. Through mission play, for example, professionals can assess new recruits to understand their specific strengths and weaknesses for tailored training. Most importantly, the Project Ares framework provides techniques to measure objectively different players/teams and approaches to help address the following key questions:

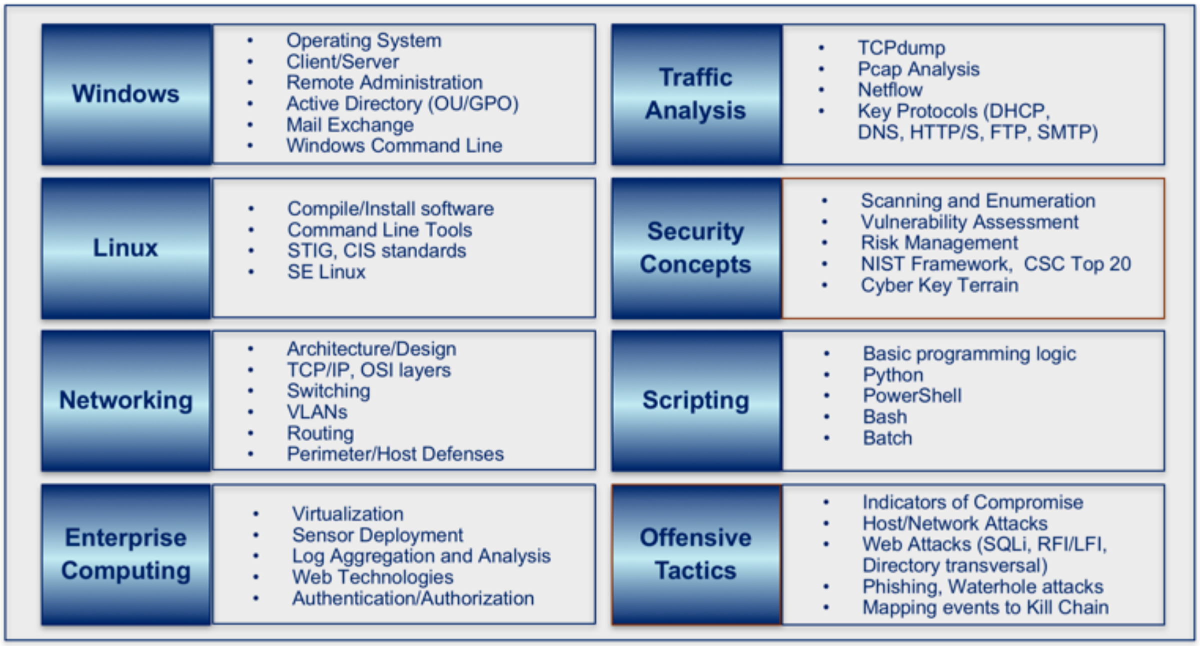
- How skilled is the current workforce?
- What work roles are necessary to meet the expected scenarios?
- How many and what type of personnel are required?
- How much training is required for them?
- Where is our curriculum falling short on subjects that staff are struggling with?
- How helpful is a new cyber tool operationally and what is the return on investment?
- What is the quantifiable cyber risk to our organization?

In answering these questions, this helps our organization better prepare for and defend against a cyber-attack.

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)?**

The increasing abundance of cybersecurity incidents brings widespread attention to the critical need to train individuals for the cyber workforce to fulfill military, government, and commercial needs across the globe. Unfortunately, academic and commercial training programs still struggle to define standard cyber work roles and career paths, resulting in confusion over the best courses or certifications that can help develop the cyber workforce needed to stem the tide of growing cyber breaches.

We derived an underlying technical core curriculum (i.e., undergraduate degree or basic training pipeline) represented in Fig. 3 by interviewing successful cybersecurity team members and asking what they were trained in (or wish they had been) that led to their success. Almost everyone said that scripting was underrepresented in core training programs but it is instrumental in automating tasks and evolving to meet a sophisticated adversary. Overall, we believe that traditional, hands-on core training is lacking in the community and instead, people are still being tested on book-knowledge and basic concepts.



Windows
- Operating System
- Client/Server
- Remote Administration
- Active Directory (OU/GPO)
- Mail Exchange
- Windows Command Line

Traffic Analysis
- TCPdump
- Pcap Analysis
- Netflow
- Key Protocols (DHCP, DNS, HTTP/S, FTP, SMTP)

Linux
- Compile/Install software
- Command Line Tools
- STIG, CIS standards
- SE Linux

Security Concepts
- Scanning and Enumeration
- Vulnerability Assessment
- Risk Management
- NIST Framework, CSC Top 20
- Cyber Key Terrain

Networking
- Architecture/Design
- TCP/IP, OSI layers
- Switching
- VLANs
- Routing
- Perimeter/Host Defenses

Scripting
- Basic programming logic
- Python
- PowerShell
- Bash
- Batch

Enterprise Computing
- Virtualization
- Sensor Deployment
- Log Aggregation and Analysis
- Web Technologies
- Authentication/Authorization

Offensive Tactics
- Indicators of Compromise
- Host/Network Attacks
- Web Attacks (SQLi, RFI/LFI, Directory transversal)
- Phishing, Waterhole attacks
- Mapping events to Kill Chain

Fig. 3. Foundation ares for the core curriculum for a cyber workforce

We believe that all cybersecurity personnel should have a solid understanding of the eight areas in Figure 3 in order to adapt to the evolving threat landscape. Once this is mastered, then specialization for one of the five positions on a Cyber Defense Team (Harden – Monitor – Pursue – Coordinate (Lead/Intel)) using any number of current commercial products, for example, should be done. With a fundamental understanding of core concepts, staff can specialize in one area and then cross-train in a secondary role. For example, the Harden personnel who must be experts in Windows, Linux/Unix and network infrastructure to include firewalls, routers, wireless access points, and printers are also typically good at host monitoring and understand the vulnerabilities in Windows OS hosts. With these skills, they could be positioned in any of the three roles (Harden – Monitor – Pursue) over their career

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?**

The US Army Cyber Protection Brigade has a concept of training and assessing cybersecurity staff from the beginning through individual certification, crew and final full team qualification. They call this a **Gunnery Table approach** that teaches core skills and moves from Gunnery Levels I to

VI. It gives the soldiers time on keyboard to learn the fundamentals and stresses how to apply the knowledge in problem solving ways versus "book" knowledge alone.

We are also supportive of the **Cyber Patriot** (https://www.uscyberpatriot.org/) and **Girls Who Code** (https://girlswhocode.com/) programs that bring cyber education in primary and secondary education. The introduction of tech/computer science in high school (and even middle school) particularly affects participation among females, because at this age teams are separate for boys and girls; most girls would not feel comfortable to gather and perform in a perceived male sport. Schools have boys and girls basketball teams but only one computer science or Cyber Patriot team, which is generally assumed to be a boys team.

Cybersecurity is a great field for women to excel in, although the statics put it at ~11% of the workforce currently (http://www.slate.com/articles/technology/future_tense/2017/03/a_new_study_suggests_the_cybersecurity_gender_gap_isn_t_getting_better.html). With so much available online, women can learn the tools and tactics on their own and build confidence in their skills before they join a team or class. If provided access to an environment that lets them learn and demonstrate their proficiency at home, then more young women will be able to feel comfortable in their abilities – even if they are then surrounded by men. The earlier we introduce the concepts, the more we portray the field as appropriate for both genders and when combined with an ability for self-learning, the more women we will see in this area of study.

For both genders, it is imperative that we focus on enabling the aptitude and energy of primary and secondary school students by providing them with the instructors necessary to teach them about ethics, discuss career paths, and reinforce that they can be "the cool kid" in cyber. Imagine the bragging rights of being on the *Varsity Cyber Team*, commensurate with being on the *Varsity Soccer Team*. Imagine a cyber arena that is equally open to male and female students to explore and build confidence in a safe and engaging manner. This is not that far reaching of a vision.

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

Primary, Secondary and University level schools need the guidelines, material and resources (e.g., hardware to run the cyber virtual worlds) to create a solid program in cyber for the US. In the US, the underlying curriculum for tech and cybersecurity is Computer Science, which is typically relegated to a single AP class in high school. It is viewed as a separate field from the Arts and Sciences and frequently portrayed in TV/media as appropriate for white/male nerds. Unless a young lady was exposed to the field earlier through a special program or perhaps from a parent role model, they are not likely to take an "Introductory" AP class in what appears to be a specialized, male-dominated field.

Schools (and society) can do quite a bit to change the perspective of all students, and particularly women and minorities, by introducing tech (and computer science) right along with "Reading, Writing and Arithmetic" in kindergarten and making it an all-purpose (everybody) skill. There are methods available today that enable primary school students to understand coding and logic, long before they grow up to think it is a difficult or uncool area of study. Although there may be a shortage of qualified teachers in the subject, there is so much available online and through sponsored activities that this can and should be adopted in primary education as the norm and encouraged in self-study.

Schools should also adopt a broader description of tech as being part of the Arts and Sciences and not separate. Computer science and cybersecurity have a very strong component of art – and not just in terms of graphic design or game development – but rather the notion that problem solving in cyber is an art form. Success requires thinking about the problem in different ways and exploring concepts that aren't rote memorization. When tech and computer science is portrayed as a *mainstay* skill, applicable across fields and not a stove pipe that is a different path from Art and Sciences, the younger generation can learn how to use those skills to succeed in several different career choices.

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)?**

We believe that there is still a great deal to do on "basic" IT enterprise cybersecurity defense training but we, at Circadence, are now more focused on developing Industrial Control Systems (ICS) mission scenarios. ICS's dominate our critical infrastructure sectors. Our goal is to have complete industries connected in a cyber "city" to enable leaders to understand the interdependence of the technologies and trust relationships. This requires additional training and specialization for the workforce and is a good stepping stone to scenarios involving the Internet of Things (IoT).

We also believe that the field of Artificial Intelligence is critical in cybersecurity. We are heavily invested in the development of Machine Learning techniques that can use the data collected from cyber training to develop models that can be used in force augmentation systems. This will result in a more effective human/machine approach.

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?**

   The work NIST performs in this area continues to be vital for the cyber community. We recommend that the NCWF be revised further to include the concepts of teams (Defense, Offense, IT, Legal/Exec), as the current 52 work roles appear to hinder the successful workforce development and performance of teams.

   The Federal level should also begin supporting the development of virtual training environments for critical assets (this could be done state by state to represent the industries on which each relies). These environments are the basis of training scenarios like we develop and use in Project Ares. Transportation, Finance, Energy, etc. all have cyber information sharing mechanisms but those can be greatly enhanced with scenario and threat emulation sharing in scenarios that deliver training. Creating "generic" representations of critical infrastructure in training environments can help bring technical experts together without concern for proprietary data.

ii. At the state or local level, including school systems?

Each state should identify its key cyber terrain and work with its National Guard cyber protection teams to train on virtual environments representing the key terrain. This would provide the states with a cyber risk assessment of their critical infrastructure and build a mechanism for National Guard defenders to interact with key industry and government personnel.

The academic community (with industry and government support) needs to help identify programs, materials and resources for schools to introduce and teach core concepts in cybersecurity no later than at the middle school level.

iii. By the private sector, including employers?

One of the barriers to quality, immersive cybersecurity training is having the virtual cloud infrastructure (Hardware) to conduct safe training. Industry should support the goal of having resources for all levels of education by sponsoring school access.

iv. By education and training providers?

Cybersecurity education and training providers need to continue to collaborate and share information willingly to help the community. Circadence is a partner with leaders such as Palo Alto Academy and several high schools and universities to bring our platform into the hands of the next generation cybersecurity professional.

v. By technology providers?

In order to provide rich, immersive cybersecurity training environments, we create virtual worlds with real-world tools. This allows students to have practice with the latest threat intelligence platform, SIEM, end-point protection or next-generation Firewall. Technology providers, such as IBM, McAfee, Cisco and Palo Alto have been generous in helping to provide virtual devices for training. Some technology providers have not yet seen the value of enabling students practice with real solutions but we hope more will support this critical need.