National Cybersecurity Workforce Framework, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" Comments on Executive Order 13800	**NIST Part I - Request for Information**	**Glenn A. Merrell, Certified Automation Professional**

Subject Area / Question	Response (*GAM-CAP*)	Priority	References	Comments (*GAM-CAP*)
General Information				
#1. Are you involved in cybersecurity workforce education or training (e.g.,curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)? Note: Providing detailed information, including your specific affiliation is optional and will be made publicly available. Commenters should not include information they do not wish to be posted (e.g., personal or confidential business information) and are strongly encouraged not to include Personally Identifiable Information in their submissions.	Yes, as Workforce Development Director for ICS-ISAC, and as a Cross Sector Industry Consultant for Industrial Automation Control Systems (IACS) Operational Technology (OT) for CIP, and as a Standards Committee Member contributing to Global IACS Cyber Security and ICS Safety Standards.	High	ICS-ISAC.org; ISA.org	
Growing and Sustaining the Nation's Cybersecurity Workforce	*Narrative Introduction in Comment column …*	Critical	For the purposes of this response: **Critical Infrastructure Protection (CIP) Sectors** = 18 as defined by the Federal Emergency Management Agency – FEMA. The Presidential Policy Directive – 21 (PPD-21) and DHS define 16 CIP Sectors	This Respondent notes that this RFI primary focus specifically addresses the relevancy and competency of the workforce toward Critical Infrastructure Protection (CIP). This must include how the Workforce Development will effect all eighteen (18 FEMA) sectors of the Critical Infrastructure, not a narrow focus of IT, but more to encompass the far broader focus of the convergence of IT and OT competencies to be leveraged toward all CIP Sectors Cyber Security.
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?	**Automation Federation –** the creator of the US Department of Labor Automation Professionals Competency Models, encompassing IT and OT disciplines and competencies in Cyber Security; **US Department of Labor – Competency Models** - these Models are comprehensive within each Competency area); **SANS – Primarily IT**, (*deficient in Operational Technologies contained in 16 of the 18 Critical Infrastructure Sectors*) ; **NICE Framework** (*deficient in Operational Technologies contained in 16 of the 18 Critical Infrastructure Sectors*); **ISA Training Curriculum for Automation Professionals –** *comprehensive across each level of competency* – modeled upon the US Department of Labor Competency Models for Automation Professionals. - ***Improvements:*** – For Cyber Security Professionals in the Critical Infrastructure, central Information Sharing and Analysis Centers (ISAC) must be securely linked with government, Research labs and Educational centers for disbursing vulnerabilities and solutions to exploits. A current ranking and notification system exists in DHS through US-CERT	High		***Note:*** *the Automation Federation competency models are available on the Competency Model Clearing House – CarrerOneStop website at https://www.careeronestop.org/CompetencyModel/competency-models/automation.aspx ISA is the administrator of the single most important Global standard for Industrial Automation Control System Cyber Security for the Critical Infrastructure (ISA99/IEC26443).*

Subject Area / Question	Response (*GAM-CAP*)	Priority	References	Comments (*GAM-CAP*)
2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?	**No.** There is a significant gap in understanding the differences between IT Cyber Security and OT Cyber Security as required in the 18 – FEMA (16 PPD-21) Critical Infrastructure Sectors, and the is significant disagreement among agencies and organizations on the approaches and KSA's required for CIP Cyber Security across all 18 CIP sectors.	Critical		
3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?	Not in my experience Excepting the Regulated, Monitored, or Defense Sectors of the Critical Infrastructure - Current practices and policies established in the remaining CIP sectors are typically insufficient, not falling under Governance of Risk Management, MoC or Continual Improvement. Additionally most practices and policies are deficient in forensics toward root-cause analysis, disbursing the findings and recording and evaluating effectiveness of solutions.	Critical	DHS ICS-CERT, Automation Federation, International Society of Automation, US Department of Labor Competency Models, DHS Critical Infrastructure Partnership Advisory Council (CIPAC)	Good Practice documents exist but are not applied.
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)?	A company *need* is entirely dependent on where the company falls within the 18 CIP Sectors and the span of the Company Enterprise portfolio. If the Company is entirely IT in nature with no physical Operational Technology Enterprise – such as Banking / Financial, the company requires KSA's specific to IT. If the Company has a mix of Data and Physical Operational Technology, then the company requires KSA's converging both IT and OT disciplines. A Company having a combination of both IT and OT cannot and should not realistically expect the IT KSA's to cover OT KSA's – encompassing Essential Health and Safety (EH&S) being Physical Vulnerabilities and Physical Hazards and Physical Risks. These expectations are not in line with current KSA's for the existing workforce or students in the pipeline. IT KSA's focus on ACCESSIBILITY in a virtual world of bits and bytes – data and databases. OT KSA's focus on AVAILABILITY in a REAL Physical world of energy-movement-temperature-pressure-level-flow with bits and bytes controlling the physical world, a.k.a. the Physical Sciences. In addition, Educational Institutions must consider the entry level aptitude of the trainee toward becoming fully competent in the required KSA's	Critical	DHS ICS-CERT, Automation Federation, International Society of Automation, US Department of Labor Competency Models, DHS Critical Infrastructure Partnership Advisory Council (CIPAC)	
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?	In the majority of the Critical Infrastructure Sectors, OT is the dominant discipline with IT being a component. The most effective Cybersecurity Education for Critical Infrastructure then exists when Educational curriculum converges IT Cyber Security methods as a component into the Physical Sciences in OT. As Such, Engineering curriculum and targeted third party specialized programs converging IT into OT must have immediate focus and priority for the development of competencies for Cyber Security toward Critical Infrastructure Protection.		ISA.org, DHS ICS-CERT, Automation Federation, International Society of Automation, US Department of Labor Competency Models, Critical Infrastructure Partnership Advisory Council (CIPAC)	
6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?	The rapid pace of evolving technology that does not apply good practice Cyber self protection, coupled with the time-to-market of KSA's into curriculum are the greatest challenges.	Critical		

Subject Area / Question	**Response (** *GAM-CAP***)**	**Priority**	**References**	**Comments (***GAM-CAP***)**
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)?	As Accessibility increases through the application and expansion of these technologies, vulnerabilities and exploits will increase in direct proportion – or at a potentially higher ratio. Education, Training and workforce development must evolve into self protection techniques and situational awareness training in all levels of society where computer technology is applied, when it is applied whether as an end user or technology developer.			
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	In general, foster programs that bring together governments-national-state-local, public and private sector agencies and groups for information sharing and collaboration toward continuous improvement applying State-of-the Art research among trusted participants in all CIP Sectors toward CIP. Applying Good Practice through timely and accurate information sharing is crucial to CIP. Certification programs that exceed the US Department of Labor Competency Models promoting demonstrated competency KSA's with relevant experience should be highlighted and promoted.			
8.i. At the Federal level?	NICE Framework is solely IT focused and is *inadequate* to apply accurately across the entire CIP; it does not apply across the majority Critical Infrastructure for OT. The framework either needs to become inclusive with all competency models prevalent in all CIP sectors – or reduced to solely IT focus.			
8.ii. At the state or local level, including school systems?	Science, Technology Engineering and Math (STEM) programs such as *FIRST® (For Inspiration and Recognition of Science & Technology)*,must be fully funded, widely applied leveraging industry professionals and rewarded with scholarships from an age where the end user is interacting with technology and is displaying an interest and aptitude, certainly where there is a clear demonstration of critical thinking.	Critical		
8.iii. By the private sector, including employers?	Every employee must be educated, evaluated and continuously updated on protecting the Company Enterprise Critical Infrastructure and maintaining situational awareness whether or not their position is directly impacted by Cyber Security.	High		
8.iv. By education and training providers?	Competency with aptitude in application of the knowledge gained from areas of training relative to the final degree or certificate must be evaluated and continually updated as Life-Long-Learning and Continuous improvement.	High		
8.v. By technology providers?	Any technology applied within the Critical Infrastructure must be certified compliant with Regulations and standards that apply to that Critical Infrastructure Sector, and at minimum, with the relevant good practice guides of the technology where the technology might affect any parameter of the application tied to protection of the environment, personnel or data. Non-compliant technology represents a potential vulnerability and risk to the CIP, and under Product Liability laws the producer and end user must both be held liable for damages caused when applying non-compliant technology.	High	ISA, ANSI, IEC, ISO, IEEE, NIST, USC / CFR, EU/CE Directives, Global Codes, Global Standards, national and local laws.	