



Reply to Request for Information (RFI) - *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development*

DOCUMENT CITATION: 82 FR 32172
DOCKET NUMBER: 170627596-7596-01
DOCUMENT NUMBER: 2017-14553

2 August 2017

SANS INSTITUTE
8120 Woodmont Avenue, Suite 310
Bethesda, MD 20814 USA



Executive Summary

The SANS Institute (<http://www.sans.org/>) respectfully submits this independent Operational Technology-focused response to the National Institute of Standards and Technology (NIST) Request for Information (RFI) relating to the NIST National Initiative for Cybersecurity Education (NICE) program that will help define policies associated with the support of Executive Order 13800 (Executive Order) dated 11 May 2017.

Through this RFI response process, SANS expresses its interest as a professional global educator that already provides information technology (IT), operational technology (OT) and IT/OT workforce cybersecurity education and training solutions to individuals, companies and Federal, state and local government entities, to participate and provide its input and leadership toward this process. SANS's response also emphasizes its continued attention to help industry address cybersecurity challenges emerging with the Internet of Things (IoT) and Industrial IoT (IIoT) as these movements effect OT systems and require new skills and capabilities in the current and future workforce to successfully mitigate associated risks.

The nature of safeguarding and securing OT systems benefit from an educated and technically trained workforce, rather than relying exclusively on written policies or imposed regulations directed at companies and an industry. SANS also sees great importance in the development of a workforce that can work across IT/OT convergence that bring together engineering & automation professionals and cyber security professionals to successfully reduce risk. SANS industry partners identified this importance to build bridges across organization boundaries and the result was the Global Industrial Cyber Security Professional (GICSP) certification. Our experience training industry leaders and practitioners in developing cyber security programs, enhancing cyber defenses, improving security testing, investigating and responding to cyber incidents has helped to illuminate the following observations:

1. Calculated investments in *people* to educate and train can have a marked improvement on the security posture of systems.
2. Given a history of incidents and attacks, and knowledge of the threat landscape, the need for cybersecurity education for most of today's workforce is essential; however, the specific type, scope, approach and regularity of such education and training must be carefully considered.
3. Formal development and extended accreditation of a course and program to certain standards can help ensure the quality and integrity of the institution, materials, instructor and administered education instruction thereby making the measure of course participation highly relevant.
4. Individuals and companies alike often benefit from consultative guidance and assistance to conduct a cybersecurity needs-analysis, review the results and establish a strategy to tailor cybersecurity education programs to the variety of roles and responsibilities.
5. The OT aspects of most small, medium and large businesses less frequently include any form of formalized cybersecurity policies to require employee security awareness (typically administered as computer-based training), basic levels of security education and training or particular understanding of cybersecurity risks to OT systems. This contrasts with *worker safety training* that for the most part has wide-spread cultural acceptance, is adhered to and enforced in the OT workforce.
6. A challenge the OT industry faces comes with the combination of *available time* and *budget* to educate its existing and incoming workforce. Both are substantial hurdles, and substituting low-cost, sub-par training or shorter or too-highly-compressed training often results in ineffective results, wasted investment, tainted views of the overall value and effectiveness of education and false senses of security—all of which can regularly lead to greater levels of security risks for companies.



7. To be an effective cybersecurity professional, it is paramount to have some foundation of at least the fundamentals of system administration, networking, architecture, basics of product design and coding approaches and basic technical skills relating to security concepts essential to understanding and addressing risks to contemporary digital and cyber physical systems.
8. For IT, OT and the IT/OT domains, in SANS' experience, it is essential that a variety of immersive educational modalities delivered by industry experts in their fields to best reach students and have a desired effect of increasing a student's knowledge and skills.
9. It is very beneficial to establish a *before* and *after* benchmark view of student's capabilities to determine cybersecurity education effectiveness. Skills-assessment tools administered before a learning experience that highlight one's strengths and opportunities for growth not only help ensure that students match education investments to their needs and capabilities, but also provide the means to measure this before and after results of the educational investment.
10. Education and training courses need to constantly evolve to reflect what is current and relevant including new technologies that emerge and the challenges they present; sometimes educational tools are retired and replaced; instructors come from industry and are security professionals that remain active in industry; the experiences of students and market needs and demands steer course direction; new guidelines, best practices, standards, regulations, policies all affect the educational products in use and in development.

As noted and ordered by the Executive Order in Sec. 3 - *Cybersecurity for the Nation*, and further underscored in subsection (d) *Workforce Development*, "in order to ensure that the United States maintains a long-term cybersecurity advantage" it is critical to "jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education," and to provide "findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity work-force in both the public and private sectors." Furthermore, the process to identify and "review the workforce development efforts of potential foreign cyber peers in order to help identify foreign workforce development practices likely to affect long-term United States cybersecurity competitiveness" are similarly essential to "ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities."

It is recognized by SANS that this collective effort to develop and execute this Executive Order will require successful collaboration among many parties including the US Government and its respective agencies, a variety of state and local government entities, other private entities and organizations as well as many individuals and companies that own, operate, service and support combinations of converged IT and OT systems is use in US critical industrial and infrastructure systems. This collaborative prospect in particular is embraced by SANS given its long-standing history that spans nearly three decades that has already positively affected more than 164,000 alumni security professionals across all industry sectors. As such, SANS Institute is pleased to participate in this effort and hereby represent the company's broad cybersecurity education and workforce development and delivery capabilities, including our professional expertise that can come to bear in support of this RFI process as directed by Executive Order 13800.

2 August 2017



Background on SANS Institute

SANS Institute was established in 1989 as a cooperative research and education organization. Its focus includes providing information technology (IT) and operational technology (OT) security training and security certifications around the world. SANS' education and training programs have created more than 165,000 alumni, with more than 97,000 people to date having also earned professional and accredited certifications across a spectrum of security disciplines. Today, it reaches over 30,000 students annually, building people's cybersecurity and risk management skills while also including them in the SANS extended community of more than 450,000 security practitioners across all industry sectors and segments. SANS also develops, maintains, and makes available at no cost, the largest collection of cybersecurity research documents and it operates the Internet's early warning system—the Internet Storm Center (<https://isc.sans.edu/>).

Everyday SANS helps companies and individual security practitioners learn and build contemporary and highly relevant security skills through formal educational tools to help people and companies more effectively address cybersecurity risks and challenges. SANS helps individuals and companies fulfill business objectives and ensure digital and cyber physical systems continue to provide adequate and higher levels of safety, reliability, availability, and productivity from those information technology (IT) and operational technology (OT) systems that make, move and power the digital world. Such digital and cyber physical systems are employed across the range of industries spanning all 16 critical infrastructure sectors and key resources (CI/KR) as defined in Presidential Policy Directive 21 (PPD-21) and the many other digital and cyber-physical systems that fall outside the purview of Department of Homeland Security (DHS). Most all of these systems employed across industry and owned and operated by private companies and local, state and the Federal government. Through SANS' collaboration and cooperation with each of these entities, it actively helps train those people who serve as an essential security ingredient to the successful development, deployment, continuous operation and improvements of comprehensive cybersecurity programs needed to safeguard and reliably operate these systems.

SANS' expert opinion is that cybersecurity education and training is most effective when developed and delivered by professional, certified educators and instructors that carry years of industry experience, direct experiential knowledge, feature unique expertise, and a demonstrable innate capability to educate, inform and motivate people to learn complex, often abstract concepts that relate to cybersecurity matters affecting people, companies, communities, citizens, the country, and the national and global economy.

Recognizing that the individual educational needs of each student and company often differ, and the most effective means to teach and learn similarly differ, SANS believes it is essential that a variety of immersive educational modalities be employed for effective education and training. Such approaches provide a tailored solution that allows individuals to choose their own path for how to receive education and training. For instance, a student may desire to learn at their own pace, learn from a live or recorded instructor, learn in a private or classroom environment, learn in a group setting or as an individual, learn through entertaining mediums, and to also have an opportunity to engage other cybersecurity experts and peers in active dialog to gain deeper insights and knowledge as part of a comprehensive learning experience. It is important that educational solutions not be too rigid and try to accommodate such needs.

As the world's leading cybersecurity educator, SANS continues to invest countless millions of dollars, significant time and intellectual capital to develop and maintain the most relevant, effective, and up-to-date cybersecurity training products available today that span educational modalities and serve most every industry sector and represent the result of a SANS commitment that started nearly 30 years ago.

SANS promotes a position that cybersecurity education and training is a core tenet in the successful design, operation, maintenance and administration of all legacy and contemporary digital and cyber physical



systems, including IT, OT, IT/OT converged systems and other systems used in critical infrastructure applications such as industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, combinations of other control systems used in process automation (PA) and manufacturing automation (MA) applications and personal, light-industry and commercial systems.

More than a 13 years ago, SANS Institute established industry's first ICS CYBERSECURITY SUMMIT AND TRAINING event to reach and educate the established and growing IT, OT and IT/OT communities. The event has directly touched thousands across industry and has continued every year since, with the upcoming March 2018 event to mark its 13th anniversary.

Additionally, SANS supports industry demands for demonstrating tangible measures of the value and effectiveness of education and training solutions, including aligning its courses and instruction to the requirements needed to obtain professional and accredited certifications and certificates-of-completion, both of which help demonstrate comprehension of a security domain and quality of educational products.

For example, SANS actively collaborates with the Global Information Assurance Certification (GIAC) organization (<https://www.giac.org/>) to align SANS' education and training products with requirements established by GIAC for more than 30 professional and accredited certifications that have allowed more than 97,000 recipients to date demonstrate mastery in critical, specialized cybersecurity domains. GIAC Certifications meet ANSI/ISO 17024 standards, align with the NICE framework and many have gained approval for DoDD 8570 Baseline Information Assurance as part of the DoDD 8140 Directive and Framework that requires Department of Defense personnel and contractors to obtain security certifications and credentials in their work area specializations. This DoDD approval is applicable for roles that interact with digital technologies and systems, including information technology (IT) systems and operational technology (OT) cyber physical systems. In addition to GIAC, SANS also provides expert education and training to prepare individuals to fulfill requirements for other relevant cybersecurity certifications and certificate-of-completion programs administered and managed by other entities.

In 2013, SANS undertook an effort with GIAC and the direct support and collaboration of owners and operators, manufacturers, suppliers, integrators, security consultants and other industry representatives to form the first-of-its-kind IT/OT cybersecurity professional certification called the GIAC Global Industrial Cyber Security Professional (GICSP™). The GICSP serves as a foundational certification of skills needed to help secure operations and infrastructures as IT and OT systems converge and cyber risks and threats emerge and evolve—to date, over 1,400 individuals globally have already earned the certification. GIAC has also launched the GIAC Response and Industrial Defense (GRID™) certification as the newest addition to its ICS portfolio and more IT and OT oriented certifications are also planned for the future.

Cybersecurity compromises and breaches to many digital systems that include an OT and cyber physical constituent system can result in direct and indirect consequences that span both the information and physical space, often with impacts that inflict disruption, damage and even destruction to equipment while sometime affecting a broad range of victims such as asset owners and operators other associated employees and personnel; localized and sometimes even decentralized business operations; other citizens and communities that depend on safe, available and reliable ICS operations; national defense; local, state, national governments; and even the national and global economy if significant enough.

For these reasons, SANS chose to established itself as the world's leading educational institution focused on cybersecurity and it advocates training and education programs be sought after, defined, adopted, sustained and maintained by individuals and companies that seek to identify, protect, detect, and respond to cybersecurity risks, recover from incidents and attacks and position to measure, monitor and mitigate such cyber risks everywhere possible through the development of a cyber-skilled workforce that evolves as cyber risks and threats evolve.

Operational Technology (OT)

Information Technology (IT) is an often-used and fitting term to describe business enterprise systems that move necessary data in order to support business-level operations and interactions; however, for many companies the core function of their operations are very tangible and circulate around manufacturing, processing and providing something physical and real to their customers and all dependent on the resulting goods and services they provide. This is the realm of Operational Technology (OT).

Operational Technology (OT): is a domain complementary to information technology (IT) that consists of hardware and software components and systems (ranging from small control systems to complex, highly sophisticated geographically distributed control systems) that when assembled make, move and power the world by combining physical and mechanical systems with digital capabilities that safely and reliably control, measure, monitor, protect, produce and deliver goods and services on which society relies.

OT systems are the core element of Cyber-Physical Systems (CPS) as defined by NIST that “are co-engineered and interacting networks of physical and computational components. These systems provide the foundation of critical infrastructure, form the basis of emerging and future smart services, and improve the quality of life in many areas.”

Today, no industry sector nor segment is untouched by the influence of OT and they all use technology to communicate, control, configure, and collect data from nearly every corner of the systems—Energy, Water, Transportation, Manufacturing, Defense as well as other cyber physical systems that often go unseen like building and environmental systems, public infrastructure, logistics, shipping, entertainment, medical, healthcare, light-industrial and the consumer space. While there are IT and OT domain similarities between, there are also differences and unique challenges to the operation and management of OT cyber physical systems that result in needs for directed cybersecurity education and skills-building training programs:

NIST Security Comparisons: IT and Industrial Control Systems

CATEGORY	IT SYSTEM	OT SYSTEM
Primary Players	<ul style="list-style-type: none"> ▪ CIO, computer science grads, “WinTel geeks,” younger generation 	<ul style="list-style-type: none"> ▪ Engineers, technicians, production managers and staff, older staff who moved “up through the ranks” from line operator to technician
Primary Focus	<ul style="list-style-type: none"> ▪ Data confidentiality and integrity ▪ Automating business processes ▪ Information management and manipulation 	<ul style="list-style-type: none"> ▪ Safety and protection of the process ▪ Response to human and other emergency interaction is critical ▪ Controlling physical processes
Component Lifetime	<ul style="list-style-type: none"> ▪ 3 to 5 years 	<ul style="list-style-type: none"> ▪ 15 to 20 years
Security Approach	<ul style="list-style-type: none"> ▪ Confidentiality, integrity, availability 	<ul style="list-style-type: none"> ▪ Availability, integrity, confidentiality
Performance Requirements	<ul style="list-style-type: none"> ▪ Not real-time ▪ High throughput demanded ▪ High delay and jitter may be acceptable (e.g., video) 	<ul style="list-style-type: none"> ▪ Real-time ▪ Response is time-critical ▪ High delay and jitter is not acceptable
Data	<ul style="list-style-type: none"> ▪ Complex data type ▪ Multilayered analytics ▪ Low data rate (10K messages/second) 	<ul style="list-style-type: none"> ▪ Simple data type ▪ Just-in-time analytics ▪ High data rate (1M messages/second)
Interfaces and Networks	<ul style="list-style-type: none"> ▪ Web browser ▪ Keyboard ▪ TCP/IP-based ▪ Typical IT networking practices 	<ul style="list-style-type: none"> ▪ Human-Machine Interface ▪ Sensors ▪ Coded displays and touch screens ▪ Serial-based (moving to TCP/IP)
Change Management	<ul style="list-style-type: none"> ▪ ITIL processes are appropriate. Software changes applied in a timely manner. Patching procedures often automated 	<ul style="list-style-type: none"> ▪ OT outages must be planned and scheduled days/weeks/months in advance. Patching reboots difficult to schedule and negatively impact productivity
Managed Support	<ul style="list-style-type: none"> ▪ Allow for diversified support styles and vendors 	<ul style="list-style-type: none"> ▪ Service support usually via a single vendor
Component Location	<ul style="list-style-type: none"> ▪ Components usually local ▪ Easy to access ▪ In controlled temperature environment 	<ul style="list-style-type: none"> ▪ Components can be isolated, remote ▪ Require extensive physical effort to gain access ▪ In high/low temperature, high-humidity environments

SOURCE: NIST SP 800-82, REV. 1, GUIDETO INDUSTRIAL CONTROL SYSTEMS SECURITY



Risk calculations in OT systems must account for potential impacts in scope and at scales greater than in IT environments. It is common and often required for OT risk equations to include considerations for potential loss of life, ecological damages, consequences from lost production and operation, business-to-business impacts and many other tangible and cascading factors. For both IT and OT domains, cybersecurity poses significant challenges; however, for OT systems, priorities, processes and response and recovery procedures established to safeguard systems and respond to incidents and attacks differs.

Today's OT workforce tasked and responsible for designing, building, operating and maintaining engineered cyber physical systems are not just automation & control system professionals. Their roles include responsibilities as architects of resilient, networked systems that connect with other systems. They must be educated and trained to interact with IT, or take on characteristics of an IT skillset since industrial control system architectures have evolved to share similar characteristics with business enterprise architectures.

Given the hybrid responsibilities for automation professionals to complement skills with cybersecurity capabilities, SANS collaborates with the non-profit AUTOMATION FEDERATION (AF) organization (<http://www.automationfederation.org/>). SANS is AF's seventh working group and works with the organization, its members and other working groups to bring together cybersecurity education for the industry's workforce to the science and engineering of automation technologies and applications.

OT engineering and technician roles also include responsibilities beyond the information technology role—OT must safeguard and harden systems from failures, accidents, physical and cyber-attacks that can disrupt, damage or cause destruction, sometimes in a widespread manner, yet these same OT personnel must also fulfill business objectives for productivity, profitability, and mandatory regulatory compliance requirements.

As such, SANS' OT-specific education and training capabilities have expanded significantly in the past 13 years since it held its first ICS Cybersecurity Summit and Training event. Since inception, SANS has assembled thousands in subsequent Summits and tens of thousands in a variety of IT, OT and IT/OT-specific education and training activities to help address the unique challenges that have emerged as industry convergence leads to cyber physical, hyper connected systems. SANS has worked with industry to develop first-of-its-kind IT/OT-relevant cybersecurity certifications with professionals already well established in the workforce. SANS continues to analyze industry to characterize the security trends, challenges and ever-changing cybersecurity risk landscape for OT, openly sharing this research information for the betterment of all of industry. SANS also continues to work with veterans and women minorities to help bring a greater supply of cybersecurity talent, skills and capabilities and diversity into today's workforce.

Cybersecurity training and education programs are essential for these domains, yet unarguably OT poses unique and evolving challenges with risks, threats, consequences and potential impacts that eclipse the risks from IT systems. SANS not only recognizes these differences, it has embraced them to orient itself to serve industry's needs for complete workforce development programs that treat companies not as separate entities partitioned into IT and OT domains, but rather as one holistic Enterprise.

SANS Institute's response to this RFI provides an expert Operational Technology perspective that spans the IT, OT and the converged IT/OT domains and IoT and IIoT industry movements that are ever-present across industry and now inextricable embedded and affecting industry and society.



Reply to Request for Comment

The responses expressed herein are perspectives, observations, and points of view of SANS Institute gained from globally serving tens of thousands of individuals and customers across most every industry sector, segment, digital and cyber physical application type.

SANS Institute hereby provides the following responses to this RFI for consideration by NIST and other relevant US Government agencies to support this RFI process as directed by Executive Order 13800. The following questions and answers directly address those as called for in this NIST NICE RFI:

General Information

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

Yes. Everyday SANS helps companies and individual security practitioners learn and build contemporary and highly relevant security skills through formal educational tools to help more effectively address cybersecurity risks and challenges necessary to fulfill business objectives and help ensure adequate and higher levels of safety, reliability, availability, productivity from information technology (IT) and operational technology (OT) systems that make, move and power the digital world.

SANS Institute (www.sans.org) was established in 1989 as a cooperative research and education organization. Its focus includes providing information and operational technology security training and security certifications around the world. SANS' education and training programs have created more than 165,000 alumni, with more than 97,000 people to date having also earned professional and accredited certifications across a spectrum of security disciplines. Today, it reaches over 30,000 students annually, building people's cybersecurity and risk management skills while also helping them join the SANS extended community of more than 450,000 security practitioners across all industry sectors and segments. SANS also develops, maintains, and makes available at no cost, the largest collection of cybersecurity research documents and it operates the Internet's early warning system—the Internet Storm Center (<https://isc.sans.edu/>).

By specializing in cybersecurity education, training, certification and research, SANS has developed worldwide expertise and experience in IT and OT cybersecurity. SANS also actively collaborates with the Global Information Assurance Certification (GIAC) organization to help closely align SANS' education and training products with the requirements established by GIAC for more than 30 professional and accredited certifications that have allowed more than 97,000 recipients to date demonstrate mastery in critical, specialized cybersecurity domains.

As direct evidence of SANS' industry focus, the GIAC Global Industrial Cyber Security Professional (GICSP™) certification serves as a foundational certification of skills required to secure infrastructures as IT and OT systems continue to converge and cyber risks and threats emerge and evolve—to date, over 1,400 individuals globally have already earned the ANSI accredited, DoDD 8570 approved GICSP certification demonstrating a verifiable level of mastery and understanding of key IT/OT security matters and skills. The GIAC Response and Industrial Defense (GRID™) certifications marks one of GIAC's newest additions to its ICS portfolio of professional certifications.



SANS is also an active participant and comprises a cybersecurity workforce development working group in the non-profit AUTOMATION FEDERATION (AF), recognized as “The Voice of Automation” (<http://www.automationfederation.org/>). SANS, as AF’s seventh working group, works with the AF organization, its members and other working groups to collaborate to advance the science and engineering of automation technologies and applications, and develop the workforce needed to capitalize on the benefits of automation and safeguard industrial control systems from cyberattack.

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?

The convergence of IT, OT, digital and cyber physical systems, coupled with ever-expanding interactions amongst businesses (to successfully deliver the capabilities that make, move and power the world) all continue to expand the levels of risks to which society is now regularly exposed.

There is no single comprehensive measure of the full reach, relevance and effectiveness of cybersecurity education, training and workforce development programs. Regardless, it continues to be shown in the aftermath of successful cybersecurity incidents and attacks, in cases where disruption, damage and in some cases destruction have occurred, that *people* are the most significant weakness to the adequate protection of today’s digital and cyber physical systems. The act of compromising systems and breaching or bypassing technical security controls is most often the result of a human-factor compromise via social engineering, phishing or exploiting human habits and tendencies. Add to this, complexity in technologies that often lead to unintended oversights, misconfigurations, architectural flaws and the like that often give an adversary an advantage to bypass security controls and meet their nefarious objectives.

As such, calculated investments in *people* to educate and train can have a marked improvement on the security posture of systems. Given a history of incidents and attacks, and knowledge of the threat landscape, the need for cybersecurity education for most of today’s workforce is essential; however, the specific type, scope, approach and regularity of such education and training must be carefully considered. Also, there are many other attributes suitable to measure to determine a cybersecurity program’s efficacy. These can include measures of effectiveness, quality, relevance, currency, practicality, global acceptance, perceived and actual value to employers and hiring entities, alignment with legal, ethical, moral responsibilities and social norms are some useful measures to discern level of goodness.

Cybersecurity education and training providers should be regularly scrutinized and challenged to demonstrate such traits to current and prospective clients. Furthermore, it is the strong opinion of SANS that they should also be evaluated based on criteria such as those relating to company mission, stability, longevity, reputation in industry, thought leadership qualities, agility and ability to evolve, student and alumni/graduate volume, student feedback, ongoing critical reviews of instructor, demonstrable accreditations and credentials, collaboration and partnering with industry peers, consortia, working groups and state, local and Federal governments, industry security guidelines, recommendations, security frameworks, standards development and perhaps most critically, the caliber of materials and pedigree and caliber of instructors who perform as cybersecurity educators.

One added, highly tangible measure of cybersecurity education, training, and workforce development stems from the volume of students that successfully complete some form of reputable cybersecurity education and training course or program. Formal development and extended accreditation of a course and program to certain standards can help ensure the quality and integrity of the institution, materials, instructor and



administered education and training instruction thereby making the measure of participation in the course a highly relevant measure.

To further expand on this assurance, a formal professionally developed and accredited certification that tests an individual's aptitude and understanding of concepts, facts, processes provides the best measures for effectiveness of education and training programs. Since not all students that complete courses go on to earn certifications, it is important to evaluate both measures independently but simultaneously. Furthermore, some certifications require ongoing continuing professional education (CPE) credits – tracking the number of certifications issued, those currently in force, the quantity that have been renewed, the quantity that have expired, and the number of CPEs submitted as earned by certification holders can also provide effective measures of adoption, market penetration and market value.

The above are valuable recommendations for any educator to follow, and important factors in the creation and administration of cybersecurity workforce development programs expected to be effective.

SANS Institute was established in 1989 and has accumulated significant fact-based experience and empirical evidence for how to develop, administer, maintain, and validate effectiveness of a variety of cybersecurity training curricula delivered through a variety of modalities. This includes continuously assessing market needs for types of cybersecurity education, development of specific educational products by experts, certifying instructors to extreme proprietary quality standards, continuous monitoring and process improvements of educational materials and instructors, having students measure and provide feedback on educator performance, and complementing many educational courses with accompanying ANSI accredited, often DoDD approved professional certifications. To date, SANS education and training programs have created more than 165,000 alumni, with more than 97,000 people to date having also earned accredited certifications across a spectrum of security disciplines. It reaches over 30,000 students annually providing education and training on cybersecurity and risk management skills to individuals and companies. SANS also has built an extended community of more than 450,000 security practitioners across all industry sectors and segments.

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

For the most part, the answer is no, and in general, there is not a sufficient understanding or agreement on the cybersecurity educational requirements for workforce categories. While secondary education, colleges, universities, vocational schools and the like are slowly adopting elements of cybersecurity into broader-scoped curriculums, focused minor- and major-programs relating to the field, especially of a comprehensive and truly practical use in industry continues to remain largely absent. Cybersecurity risks, threats and risk management is complex and sometimes abstract. The very nature of cybersecurity risks, compounded by particulars relating to a company's culture, its current workforce-skillset and intragroup and intergroup interactions, unique worker responsibilities all lead to challenges in defining what skills building is most needed and beneficial for its workforce. SANS' experience is that both individuals and companies alike often benefit from consultative guidance and assistance to conduct a cybersecurity needs-analysis, review the results and establish a strategy to tailor cybersecurity education programs to the variety of roles and responsibilities.

As a cybersecurity educator and prior to administering and education or training, many SANS client engagements first start with a discussion to determine personal and business objectives, needs, concerns, current capabilities, time and effort expectations, desired outcomes, definitions of success, measures of success, appropriate budgeting, long-term planning and at least a cursory skills assessment of current state as a benchmark against which to determine results. This process is formalized in the SANS CyberTalent program (<https://www.sans.org/cybertalent/>) that assesses individual and group cybersecurity skill levels



(<https://www.sans.org/cybertalent/assessment-products>). The output from these assessments are valuable recommendations for any cybersecurity educator to follow, and important factors in the creation and administration of cybersecurity workforce development programs expected to be effective.

In 2013, SANS undertook an effort with GIAC and the direct support and collaboration of owners and operators, manufacturers, suppliers, integrators, security consultants and other industry representatives to form the first-of-its-kind IT/OT cybersecurity professional certification called the GIAC Global Industrial Cyber Security Professional (GICSP™).

The GICSP serves as a foundational certification of skills needed to help secure operations and infrastructures as IT and OT systems converge and cyber risks and threats emerge and evolve—to date, over 1,400 individuals globally have already earned the certification. As a formal part of the development process for the certification, SANS and GIAC administered an exhaustive Job Task Analysis (JTA) to understand industry needs and align the certification requirements, and complementary education and training course to these specific needs.

More recently, GIAC has launched the GIAC Response and Industrial Defense (GRID™) certification as a new addition to its ICS portfolio. More IT and OT oriented certifications are planned in the future too.

Individual educational needs of each student and company also often differ. In many cases, the most effective means to teach and learn similarly differ and SANS believes it is essential to determine best-fit educational courses and programs for a particular student or group. For this reason, SANS also provides a variety of immersive educational modalities tailored towards how a student or group will best learn. Here again, these attributes are deemed valuable, if not essential recommendations for any cybersecurity workforce education program to be effective.

SANS continues to invest to understand, assess and orient cybersecurity education programs in a manner most relevant and valuable to its clients. The following chart depicts a SANS reference resource employed to help guide customer discussions about how to better determine a cybersecurity education and training strategy for its workforce:

ICS-Related Job Role Mapping

COMPETENCY LEVEL	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
Technical Leader				
Expert Knowledge				
Mastery Knowledge				
Essential Knowledge (Foundational)				
Base Knowledge (Awareness)				
JOB ROLE	USE	SUPPORT AND MAINSTREAM	SUPPORT AND MAINSTREAM	DESIGN
	All individuals who interact with Process Control Devices	Engineering, Operations Technology, IT Cybersecurity, IT Staff, Support Staff	Engineering, Operations Technology, IT Cybersecurity, IT Staff, Management	Engineering, Operations Technology, IT Cybersecurity, IT Staff

Job Role Groupings

Engineering

- Process Engineer
- Electrical, Controls, and Mechanical Engineer
- Project Engineer
- Systems and Reliability Engineer
- OT Developer
- Plant Networking
- Control/Instrumentation Specialist
- Protection and Controls
- Field Engineer
- System Integrator

Operations Technology

- Operator
- Site Security POC
- Technical Specialists (electrical/mechanical/chem)
- OT Security
- ICS/SCADA Security
- ICS/SCADA Programmer

Management

- Plant Manager
- Risk/Safety Manager
- BU Management
- C-level Management

Support Staff

- Remote maintenance & TS
- Contractors (engineering)
- IT and Physical Security Contractor
- Procurement Specialist
- Legal
- Contracting Engineer
- Insurance
- Supply-chain Participant
- Inventory Management/Lifecycle Management
- Physical Security Specialist

IT Cybersecurity

- ICS Security Analyst (level 1)
- ICS Security Analyst (level 2)
- Security Engineering and Architect
- Security Operations
- Security Response and forensics
- Security Management (CSO)
- Audit Specialist
- Security Tester

IT Staff

- Networking and Infrastructure
- Host Administrator
- Database Administrator
- Application Development
- ERP/MES Administrator
- IT Management
- Architect

Job-Level Descriptions

LEVEL 1 Essentials Knowledge

- Entry-level technical skill set
- Is capable of working under general supervision
- Requires significant day-to-day direction
- Has some tactical break/fix responsibilities
- An ability to satisfactorily complete technical training and related certifications
- Contributes to a safe work environment
- Understands company standards and applicability to job role

LEVEL 3 Expert Knowledge

- Demonstrates most characteristics of Levels 1 and 2
- Has mastered skills related to specific job responsibilities
- Has some strategic planning
- Is capable of developing functional and/or technical specifications regarding business requirements
- Consistently prioritizes workload without management intervention
- Is considered by peers and leadership to be SME in working group
- Is proactive in identifying business/enterprise technical needs
- Has a history of developing strong working relationships with peers, leadership, and customers
- Has an ability and willingness to train/coach others
- Demonstrates ownership of systems and processes
- Has an ability to express complex technical concepts effectively
- Has an ability to work well with people from different disciplines with varying degrees of technical experience
- Has an ability to interpret and apply company standards as applicable to job role and technical environments

LEVEL 2 Mastery Knowledge

- Demonstrates most characteristics of Level 1
- Has an ability to work under minimal supervision
- Has significant skills related to job-specific responsibilities
- Has an ability to address tactical break/fix situations
- Is proactive in identifying department technical needs
- Has an ability to manage small projects
- Has an ability to review and contribute to functional and/or technical specifications regarding business requirements
- Has an ability to develop application/system documentation
- Has good planning, organizational, verbal, and written communication skills
- Consistently contributes to team effectiveness and demonstrates concern for group success
- Has an ability to implement company standards as applicable to job role

LEVEL 4 Technical Leader

- Demonstrates most characteristics of Levels 1, 2, and 3
- Understands big picture and how actions affect other system interoperability
- Has excellent problem solving and decision-making skills without having all of the information
- Has knowledge of business purpose beyond own scope of responsibilities
- Demonstrates strategic-planning skills
- Has an ability to communicate with all levels of management and customers
- Has strong presentation skills
- Has an ability to manage large projects
- Has an ability to develop recommendations to address identified business issues
- Has an ability to direct other team member's daily activities

Competency-Level Descriptions

<p>Base Knowledge (Awareness)</p> <p>Training focuses on security behaviors for individuals who interact with, operate, or support Industrial Control Systems. Training program may introduce ICS, the risks or types of ICS attacks, basic system and network defenses and controls, as well as typical ICS governance and policy best practices. Program goal should change human behavior in an ICS environment and reduce risk.</p>	<p>Essentials Knowledge (Foundational)</p> <p>Training program should provide a foundational set of standard skills and knowledge for industrial cybersecurity professionals. The training should ensure that the workforce involved in supporting and defending industrial control systems are trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats. Across a diverse audience, the training program should build a foundation and ensure workers at this level develop a common language in ICS, understand the underlying theories in ICS for Safety and Reliability, and provide an overview of the basic tools for industrial control system security in settings across a wide range of industry sectors and applications.</p>	<p>Mastery Knowledge</p> <p>Training should be role specific and focus on individual and organizational needs to advance knowledge, skills, and ability in a specific field.</p>	<p>Expert Knowledge</p> <p>Training should focus on coordinated response and improvement of team capabilities. This level is typically achieved in joint exercises and projects.</p>
		<p>Technical Leader</p> <p>Training should focus on management and technical team development as well as methods for interacting with other teams and communicating technical concepts to non-technical audiences.</p>	

SANS also collaborates with the non-profit AUTOMATION FEDERATION (AF) organization (<http://www.automationfederation.org/>) to further understand the automation & control discipline perspectives and trends relating to how cybersecurity affects industry and the engineering workforce. Through this partnership, SANS and AF continue to bring greater clarity to the topic of OT cybersecurity and how critical education and training is for today's automation professionals in and entering the workforce.

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

Organizations often segment their business into Information Technology (IT) and Operational Technology (OT) domains, and most acknowledge interactions and interdependencies amongst them.

The IT aspects of many medium to large businesses typically include some form of formalized cybersecurity policies that require employee security awareness, basic levels of security education and training to build an understanding of cybersecurity risks and capability to harden the business architecture and operations against attacks. For company personnel that are not directly affiliated or responsible for the company's enterprise cyber security, such as those specifically in IT security and management roles, it remains uncommon for most companies to require immersive cybersecurity training on a broad basis.

While policies that call for some forms of security awareness programs (typically administered as computer-based training) are growingly standard and more widely administered in medium to large companies, it is common for many smaller companies to operate without any such policies and formalized program in place. Furthermore, few companies regardless of size are actively defining or enforcing measures of education and awareness program effectiveness.

The OT aspects of most small, medium and large businesses less frequently include any form of formalized cybersecurity policies that require employee security awareness (again, typically administered as computer-based training), basic levels of security education and training or particular understanding of cybersecurity risks to OT systems. This contrasts with *worker safety training* that for the most part has wide-spread cultural acceptance, is adhered to and enforced in the OT workforce. Furthermore, in the OT domain it remains fairly uncommon for most companies to write policies that define or require expansive or immersive cybersecurity training on a broad or consistent basis for company personnel who are not directly affiliated or responsible for the cybersecurity of the company's OT systems. When such training and awareness programs are administered, it is not uncommon to see them operate without specific governance to make sure there is compliance or to determine the effectiveness of the cybersecurity education and awareness programs.

The breadth of OT systems across industry sectors and segments often sees common shortcomings in the cybersecurity education and training of personnel tasked with safeguarding and operating critical systems. While there is measurable growth in the number of OT personnel seeking cybersecurity education and training, there remain particular industries, companies and departments within companies where the investment is low to nonexistent. For instance, the Energy Sector's Power & Utilities and Oil & Gas industries are more progressive at making proactive investments in OT cybersecurity education and certifications. Contrast this with Water/Wastewater industry where security investments currently rarely extend beyond physical security controls.

Some companies have become proactive to establish company policies that include specific requirements for workforce cybersecurity education and training. Because of the company's history of cybersecurity leadership, combined with market and specific client demands, SANS specifically spearheaded the development of IT/OT cybersecurity courses and worked closely with many of these industry-leading companies to create products that support these company objectives. This includes helping to assess current



worker skills so growth in competence and capabilities can be tracked over time via job task analysis activities and the SANS skills assessment tool called CyberTalent that assesses individual and group cybersecurity skill levels (<https://www.sans.org/cybertalent/assessment-products>).

Extending to skills assessments, in 2013 SANS undertook an effort with GIAC and the direct support and collaboration of major, industry-leading owners and operators, manufacturers, suppliers, integrators, security consultants and other industry representatives to form the first-of-its-kind IT/OT cybersecurity professional certification called the GIAC Global Industrial Cyber Security Professional (GICSP™). The GICSP serves as a foundational certification of skills needed to help secure operations and infrastructures as IT and OT systems converge and cyber risks and threats emerge and evolve—to date, over 1,400 individuals globally have already earned the certification. GIAC has also launched the GIAC Response and Industrial Defense (GRID™) certification as the newest addition to its ICS portfolio and more IT and OT oriented certifications are planned too.

In both IT and OT domains, these respective factors underscore the importance to provide highly relevant and effective cybersecurity education and training to IT and OT personnel whenever investments are made, rather than seeking out substandard education solutions that may end up having little to zero effect on mitigating security risks.

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)?

There is a spectrum of cybersecurity skills that are essential and others that are highly desirable in a workforce as it grows in capability, size and effectiveness.

Basic cybersecurity awareness skills, often fondly called cybersecurity “good hygiene” and “good behaviors” and practices that become a natural part of worker skillsets are skills that should ideally be innate in new hires, yet often still require education and training in order to establish a baseline. Regardless of new or existing employee, basic cybersecurity awareness skills building is an essential element to help remind and educate individuals of the company’s reliance on the employee’s vigilance as a first line of defense.

Although there are industry differences in the types of specific skills that are needed (i.e. some industries are required to adhere to regulations such as the Energy: Electricity sector and NERC-CIP), excluding those specific requirements the IT and OT cybersecurity skills most relevant to one role are often highly transportable between industries—i.e. many foundational aspects of an ICS cybersecurity skillset in one industry can be applied to another industry’s ICS.

For more sophisticated roles known to interact with mission critical systems, where risks to people, property and information are recognized, a higher degree of cybersecurity skills are necessary. In these cases, cybersecurity awareness programs should be complemented with more role-specific security training oriented around job function and role interaction with other parts of an organization.

Orienting cybersecurity education and training to how a job is expected to perform its duties is important. For instance, considering the multi-phased view of managing a security program in the context of *Identify, Protect, Detect, Respond and Recover*, the cybersecurity skills a job will need will need can differ wildly from other jobs in the company. Considering how the role maps to life cycle phases for digital and cyber physical systems (i.e. *Design, Build, Operate and Maintain*), and the skillset needed for a job can again be vastly different than other jobs in the company.



It is not uncommon for employers, including hiring managers to not adequately know what cybersecurity skills are beneficial, essential and highly valuable to their existing and evolving workforce. In some cases, there's little consideration being given to job roles regardless of levels of associated risk to an individual, company, community or a variety of other stakeholder's who depend on how a worker performs their task. In other cases, companies may be too focused on locating the perfect candidate that precisely fits a job role and security capabilities thereby leaving critical security roles altogether vacant.

Narrowing down to what cybersecurity skills are needed for a job, those that are required at the outset and those that can be acquired over time require careful consideration and many employers lack the capability and perspective to know where to start with this process.

The following matrix is an example tool that helps SANS discuss and establish high-level job requirements and how to better match cybersecurity education and training to those requirements with our clients—these often lead to valuable recommendations for any educator to follow, and important factors in the creation and administration of cybersecurity workforce development programs expected to be effective:

SANS IT/OT Job Role Cybersecurity Involvement

Job Role / Title	Functional Area	Sr. Management Visibility			IT-OT Linkage			ICS Lifecycle Involvement					Security Controls Responsibility			Risk Phase Involvement					
		Low	Medium	High	Low	Medium	High	Design	Procure	Install	Operate	Maintain	Physical	Technical	Administrative	Identify	Protect	Detect	Respond	Recover	
Process Engineers	Engineering	*				*		*	*	*	*	*	*	*	*	*	*	*	*	*	*
Electrical & Mechanical Engineers	Engineering	*			*			*	*	*	*	*	*	*	*	*	*	*	*	*	*
Project Engineers	Engineering	*	*				*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
OT Developer	OT	*					*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
PLC Programmers	OT	*			*			*	*	*	*	*	*	*	*	*	*	*	*	*	*
Emergency Operations Manager	Operations	*	*		*			*	*	*	*	*	*	*	*	*	*	*	*	*	*
OT Support Staff	OT	*				*		*	*	*	*	*	*	*	*	*	*	*	*	*	*
Plant Networking	OT	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Control specialist	OT	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Protection & Controls	Engineering	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Field Engineers	Engineering	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Operator	Operations	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Site Security POC	CyberSec	*	*		*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Technical Specialists (electrical/mechanical/chem)	Engineering	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
PC IT Security	CyberSec	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
SCADA Security	CyberSec	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
SCADA Programmer	OT	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Plant Manager	Management			*			*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Risk Manager	Management			*			*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
BU Management	Management			*			*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
C-level Management	Management			*			*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Remote maintenance & TS	OT	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Contractors (engineering)	Engineering	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Security Contractors	CyberSec	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Procurement Specialists	Support	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Legal	Support			*	*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Contracting Engineer	Engineering	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Insurance	Support	*	*		*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Supply-chain participant	Support	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Inventory Management/Lifecycle Management	Support	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
iPII Specialists-Data Specialists	Support	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
ICS Security Analyst (level I)	CyberSec	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
ICS Security Analyst (Level II)	CyberSec	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Security Engineer & Architect	CyberSec	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Security Operations	CyberSec		*		*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Security Response & Forensics	CyberSec			*	*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Security Management (CSO)	Management			*	*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Audit Specialists	IT	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Security Tester	CyberSec	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Networking & Infrastructure	IT	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Host Admin	IT	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Development	IT	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
IT Management	Management	*	*		*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
Architecture	IT	*			*		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*

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 SANS' expert opinion, to be an effective cybersecurity professional, it is paramount to have some foundation of at least the fundamentals of system administration, networking, architecture, basics of product design and coding approaches and basic technical skills relating to security concepts essential to understanding and addressing risks to contemporary digital and cyber physical systems. These fundamentals help ensure common language and understanding of security concepts, including risks, threats, probability, impacts and consequences and security processes needed to build or operate security programs that effectively identify, protect, respond and recover from incidents and attacks for instance.

The most effective means to educate one person can be different from the way to effectively educate a group. There is no one educational solution that works of everyone; nonetheless, the quality of material and the instructor whether front-and-center, or operating behind the scenes are often the most essential ingredients to help to ensure that students reach an objective of higher cybersecurity knowledge. There are also a variety of other means for cybersecurity education that expand outside of a traditional classroom perspective.

There is significant value to be gained by security professionals who obtain hands-on experience, not just classroom instruction of hypothetical situations. For this reason, broad education programs that incorporate such interactive and immersive experiences (e.g. opportunities to work with real-world tools, analyze real devices and systems), and programs taught by expert instructors with real-world experience are critical elements to cybersecurity education and training for industry.

For IT, OT and the IT/OT domains, in SANS' experience, it is essential that a variety of immersive educational modalities delivered by industry experts in their fields to best reach students and have a desired effect of increasing a student's knowledge and skills. This variety includes supporting and individual or company's desire to choose how they receive education and training that accommodates their decision to learn at their own pace, learn from a live or recorded instructor, learn in a private or classroom environment, learn in a group setting or as an individual, learn through entertaining mediums, and to also have an opportunity to engage other cybersecurity experts and peers in active dialog to gain deeper insights and knowledge as part of a comprehensive learning experience.

Cybersecurity education and training can be effectively delivered through a variety of mediums. This variety is often very necessary since some concepts are regrettably dry and are unlikely to normally generate much interest or excitement from students, yet remain important if not essential aspects to maintaining a successful security program.

For instance, the most basic cybersecurity awareness training that focuses on good security hygiene practices and how employees must practice vigilance can be highly effective when delivered in a highly engaging and entertaining manner that includes strong visuals, relevant examples and scenarios, diverse topics, thought provoking ideas, reasonable time durations, clearly communicated objectives and measureable results to track not only completion rates but also comprehension and understanding. Programs that incorporate these ingredients can be more effective in reaching personnel and ensuring they grow their knowledge from exposure to the materials. Furthermore, cybersecurity awareness programs must similarly account for differences in roles and responsibilities since the security risks, responsibilities, procedures, challenges and



responder reactions can be vastly different between personnel, especially when comparing IT roles to OT roles. For this reason, tailored cybersecurity awareness training programs designed for categories of workers can be highly beneficial, such as awareness materials directly oriented toward an end-user, a developer community and OT engineering community.

In 2013 SANS undertook an effort with GIAC and the direct support and collaboration of major, industry-leading owners and operators, manufacturers, suppliers, integrators, security consultants and other industry representatives to perform a job task analysis (JTA) of industry needs. The results lead to specific cybersecurity courses offered by SANS that are directed at IT, OT and IT/OT personnel responsible for digital and cyber physical systems. The JTA also led to the creation of the first-of-its-kind IT/OT cybersecurity professional certification called the GIAC Global Industrial Cyber Security Professional (GICSP™). The GICSP serves as a foundational certification of skills needed to help secure operations and infrastructures as IT and OT systems converge and cyber risks and threats emerge and evolve—to date, over 1,400 individuals globally have already earned the certification. GIAC has also launched the GIAC Response and Industrial Defense (GRID™) certification as the newest addition to its ICS portfolio and more IT and OT oriented certifications are planned too.

In both IT and OT domains, these respective factors underscore the importance to provide highly relevant and effective cybersecurity education and training to IT and OT personnel whenever investments are made, rather than seeking out substandard education solutions that may end up having little to zero effect on mitigating security risks.

Furthermore, the “classroom experience” remains a highly effective and popular means for education, training and learning. However, customer needs and desires as well as technology has enabled the classroom experience to evolve in a manner better suited to addressing the time, travel, learning pace, language, individual/group dynamics that would otherwise be static if classroom education was only delivered in its most traditional sense.

Effective cybersecurity training with “classroom experience” is now comprised of varying combinations and popularity of physical classrooms (led by instructors teaching a class with some form of group dynamic), virtual classrooms (electronically delivered instructor-led classes that also feature a virtual class group dynamic), on-demand approaches for students to experience in a pre-recorded digital manner instructor-led education where a student can set their own pace over a period of time to progress through materials. These approaches are not only effective at aligning cybersecurity education and training with how students can best learn, but these modalities also afford students and companies alike the capability of finding the best business-fit for how and when personnel can obtain training, minimizing business impacts and other distractions. This can be especially important for companies with OT personnel since the flexibility of companies and individuals to obtain training, including when, where and how can be restricted.

In combination with awareness, computer-based training (CBT) and classroom training (whether physical, virtual or on-demand), cybersecurity education and training opportunities should include exposure and investment in a variety of other mediums that help professionals grow knowledge, understanding and skills. Some complementary mediums can include highly IT, OT and IT/OT-combined interactive, hands-on experiences in game-like settings such as capture-the-flag activities, red-blue team competitions, competitive scoring-based events, man-vs-man, man-vs-machine events, board-game/scenario-based activities and the like, each of which can be highly effective and result in cybersecurity education and skills building in a non-traditional way. Other available mediums include exposure to cybersecurity-related research, webinars, summits, forums, conferences, symposiums and even social birds-of-a-feather type gatherings where information and discussion is readily provided and often exchanged.



There are benefits to measuring where possible the effectiveness of cybersecurity education and training, especially when determining if time and money investments result in successful increase in security skills and if these increases will equate to value for the student or company. It is very beneficial to establish a *before* and *after* benchmark view of student's capabilities to determine cybersecurity education effectiveness. Skills-assessment tools administered before a learning experience that highlight one's strengths and opportunities for growth not only help ensure that students match education investments to their needs and capabilities, but also provide the means to measure this before and after results of the educational investment.

In SANS experience, skills assessments conducted before training is administered is an important process to determine educational needs and fit and the effectiveness of the administered training—these skills assessments are equally applicable to IT, OT and hybrid personnel. An example of how SANS helps individuals and companies conduct skills assessments is CyberTalent (<https://www.sans.org/cybertalent>).

Although completing a course or a learning activity is an accomplishment in its own right, an even more demonstrable measure of educational effectiveness can be gained through a professional and accredited certification process that consistently verifies and provides assurance that a level of understanding, or successful knowledge-transfer or has taken place for a student. This helps to mark a difference between merely attending and completing a learning activity as compared to showing one has learned something.

Professional and accredited certifications that couple with specific cybersecurity courses continue to gain popularity and a growing number of students pursue a certification when available to demonstrate both course completion and level of practical understanding on a security topic. These certifications help also to communicate to others that one has fulfilled a prescribed set of requirements relating to a cybersecurity discipline

Two examples that are focused on the OT domain, ICS specifically include the accredited GIAC Global Industrial Cyber Security Professional (GICSP™) and the GIAC Response and Industrial Defense (GRID™) certifications with a current combined set of 1,450 certified professionals serving industry (<https://www.giac.org/certifications/ics>)

These are valuable recommendations for any educator to follow, and important factors in the creation and administration of cybersecurity workforce development programs expected to be effective.

Lastly, cybersecurity education and skills-building is not prevalent in K-12, STEM programs, nor in most formal college and university curriculums today, thereby lending to a direct industry need for post-graduate training in the cybersecurity and cyber risk management discipline.

In its near 30 years of experience and having already reached over 165,000 alumni, SANS has taken an approach to invest substantially to build intellectual capital and time to develop and maintain the most relevant, effective, and up-to-date cybersecurity educational products that span educational modalities and serve industry sectors and segments. Additionally, SANS continues to work with GIAC, an organization that has issued professional and accredited certifications to over 97,000 people since 1999 across a spectrum of security disciplines, while it also provides education and training solutions directly applicable to other entities that administer certifications and reputable certificates-of-completion programs.

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

The shortage of qualified, cybersecurity-skilled workers that can fill existing and new roles and tangibly help organizations transform operations is one of the largest challenges to industry and the nation. There are hundreds of thousands of unfilled cybersecurity jobs today with more emerging across all industry sectors



and many of these jobs continue to remain unfilled due to a shortage of workers with the correct skillset, as well as the public perception that industrial OT roles cannot be fulfilling or necessarily financially rewarding, leading to the few number of security-skilled workers often seeking jobs in non-industrial sectors.

A largely unknown and underappreciated reality is that today, there are ample opportunities and demands for security professionals across industry and wages for OT security positions filled by qualified security professionals continue to increase:

In a 2016 career impact survey administered by SANS that collected data from more than 700 certified security professionals, each of whom hold the Global Industrial Cybersecurity Professional (GICSP) certification, the average annual salary of a GICSP holder was \$104,000 USD. This average salary marks a nearly a 17% increase over the same group's wages reported in 2013. It also marks an average annual, year-over-year increase of 5.5% for the period 2013-2016. These same GICSPs projected their future earnings expectations for 2017 and beyond to grow at an average rate of 7% annually.

At this pace, the GICSP's salary will substantially outpace the average Automation/Control Engineer's salary increase of just over 1% seen for the period 2013-2016 as cited in Intech Magazine, Sept/Oct 2016. Furthermore, the average GICSP holder's salary in absolute dollars is projected to nearly match the average Automation/Control Engineer's salary in 2017 and surpass it thereafter.

Given the projected higher salary increase rate for GICSPs over Automation/Control Engineers, the earning capacity of this class of certified security professional will only continue to pull away from these engineers. It is important to mention that many Automation & Control Engineers are starting to recognize this trend and have started to more actively seek OT cybersecurity education, training, professional and accredited certifications like GICSP to capitalize on this trend. These trends are readily apparent in the registrations SANS sees for its ICS cybersecurity curriculum and what GIAC observes in those attempting and earning the GICSP certification.

Another challenge the OT industry faces comes with the combination of *available time* and *budget* to educate its existing and incoming workforce. Both are substantial hurdles, and substituting low-cost, sub-par training or shorter or too-highly-compressed training often results in ineffective results, wasted investment, tainted views of the overall value and effectiveness of education and false senses of security—all of which can regularly lead to greater levels of security risks for companies.

To overcome the *available time* challenges and reduce the *budget* burden, alternative approaches to traditional off-site "classroom experience" training can be highly beneficial to reduce travel time and travel expenses. This can come in the form of online training such as virtual classrooms and on-demand approaches. Another option is to seek out local community classes that help students get trained while in closer proximity to their facilities. Private classes conducted on-site are yet another option, with an added benefit that the students may all work for the same group or organization and extract even greater value from the educational experience. These alternatives can be highly effective at balancing students time and associated expenses, helping ensure best-in-class training is sought from best-in-class providers without compromise.

In some cases, progressive models for subsidizing training budgets have also emerged in industries where industry associations, consortia, working groups and other similar organizations have the capability and budget capacity to help constituents more readily obtain cybersecurity education. In these models, organizations may cover all or portion of the expenses associated with its members obtaining cybersecurity training from professional educators, thereby helping smaller organizations in particular to access these education services. These models have shown themselves especially effective in industries comprised of

many smaller entities that have limited budgets and limited staff, yet are still high-risk critical infrastructure owners and operators.

SANS' activities with AUTOMATION FEDERATION (AF) organization (<http://www.automationfederation.org/>) have brought to light similar shortcomings in finding available skilled automation & control system professionals as well as challenges with an aging workforce not being replaced in-kind with new workers as they transition to retirement. In some cases, *technology* becomes a substitute for a retiring workforce, yet this means new and current workers must carry both automation and security skills to be effective. This further adds to this list of challenges and opportunities for cybersecurity education, training, and workforce development

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)?

Technology advances can comprise both a *security blessing* and a *curse* for digital and cyber physical systems. In some cases, technology can help aid in the identification, detection and protection and recovery of systems from cyber threats, the counterarguments are that with most technology comes complexity and a need for greater connectivity and information exchange. These factors make the safeguarding and security of systems more challenging, often increasing risks for misconfiguration, failures, unknown vulnerabilities in unused or unknown services, incompatibilities or conflicts with operations both digital and workflows, greater challenges with asset management.

In some cases, the best cybersecurity controls are the least technical and have nothing to do with technology because they are steeped in investments in *people, process, policy and non-technical administrative measures and controls*. Regardless, advances in technology in cybersecurity can absolutely bring value and help mitigate risk so long as it is carefully balanced with human-factors that are unavoidable and essential element to most digital systems, and most every cyber physical system. Especially in the OT domain, as existing technologies expand in use, and as new technologies emerge that afford security benefits, the contemporary OT workforce cybersecurity needs to be aware and evolve accordingly to determine rewards and risks, costs and value, fit and function, complexity, sustainability and potential cybersecurity risk-mitigating alternatives. This requires the workforce to constantly learn and evolve, and to do so at a pace faster than the traditional OT domain has moved in the past. The result is a need if not requirement for cybersecurity education programs that evolve over time as opposed to one-off classes that may deliver only temporary value if not complemented with relevant ongoing cybersecurity education and training.

Recent testimony delivered by SANS to FERC underscores the importance of teaching existing automation & controls engineers and technicians a cybersecurity skillset to complement their existing skills. This is not only a required expansion of the job requirements for engineering and technical roles, but also capitalizes on these individuals' capabilities to learn new technologies, understand and develop solutions for often abstract, complex challenges that are already present in the systems for which they are responsible:

“Continued efforts from NERC focused on utility cyber and physical exercises like GridEx, DoE led industry cyber security training workshops, and private sector provided electricity sector specific technical, hands-on, cyber security training will continue to improve our overall capabilities and preparedness. This is an encouraging area where NERC Registered Entities are moving beyond the standards requiring awareness training towards specialized cybersecurity training for security and ICS staff.” – Prepared Statement of M. Assante Director, SANS Institute before the Federal Energy Regulatory Commission (FERC) Technical Conference on Reliability, 22 June 2017.

An automation engineering and technical staff that expands its skillset to include cybersecurity education may become a critical element to the ICS Cyber Kill Chain. This concept of automation and control system analytics as a means to help identify security threats (beyond just using this data for greater efficiency and productivity) is explored in detail in a SANS whitepaper titled DIGITAL GHOST: TURNING THE TABLES (<https://www.sans.org/reading-room/whitepapers/analyst/digital-ghost-turning-tables-37567>). Many of the engineering and technical staff currently responsible for safeguarding operations of critical infrastructure have an innate capability to identify and isolate unusual operational characteristics in automation systems that could be indicators of compromise or impending risks. The physical nature of many critical infrastructure systems blends, power, mechanics, logic, networking and software together. As highly engineered and tuned systems with many interdependencies amongst these functions, even a minor change, authorized or not can show itself in other aspects of operation. This means, cybersecurity threats may first show themselves in different, potential unusual or erratic behavior of a system long before traditional security controls might see any indicators of change or compromise.

The need for cybersecurity education to evolve matches the need for the skills of cybersecurity professionals to similarly evolve along with technology. New risks emerge and threat actors targeting industry continue to demonstrate creativity and agility to circumvent new and existing security technologies, capitalize on the exposure resulting from highly connected, complex systems and the human-element, i.e. *people* who are the weakest link (yet potentially strongest security element) in a system.

For IT/OT and pure OT systems, SANS strictly follows an approach it recommends all education programs adopt. Education and training courses should constantly evolve to reflect what is current and relevant including new technologies that emerge and the challenges they present; sometimes educational tools are retired and replaced; instructors come from industry and are security professionals that remain active in industry; the experiences of students and market needs and demands steer course direction; new guidelines, best practices, standards, regulations, policies all affect the educational products in use and in development. Some examples where these practices are apparent are in the SANS ICS cybersecurity curriculum (<https://ics.sans.org>) and the GIAC ICS-oriented certifications (<https://www.giac.org/certifications/ics>).

Specific to the certifications, the accredited GIAC Global Industrial Cyber Security Professional (GICSP™) and the GIAC Response and Industrial Defense (GRID™) certifications have a current combined set of 1,450 certified professionals serving industry. Neither of these certifications, nor others in the GIAC portfolio are static. Once a professional earns a certification, that professional must obtain and maintain a continuous professional education (CPE) credits to help ensure and encourage personal education and knowledge-building will continue long after a classroom experience and success initially earning a professional certification. The CPE element in particular is an important mechanism that can help facilitate and encourage a cybersecurity educated workforce to keep pace with technology advances in addition to industry change.

There is also significant value to be gained by education programs that include hands-on experience, not just classroom instruction of hypothetical situations. Broad education and training programs that incorporate interactive and immersive experiences with existing, new and innovative technologies (e.g. opportunities to work with real-world tools, analyze real devices and systems) and taught by expert instructors with real-world experience are crucial to effective cybersecurity education for industry.

The above are valuable recommendations for any educator to follow, and important factors in the creation and administration of cybersecurity workforce development programs expected to be effective.

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?

It is SANS Institute's recommendation that Federal programs focus on helping ensure tomorrow's workforce is gaining the necessary cybersecurity awareness and skillset to be effective as it enters the workforce. This includes working with, empowering and supporting states and local governments to establish and expand K-12 and STEM programs to include particular focus on cybersecurity best-practices relevant to protect a citizen, but also to be applicable to industry as they enter the workforce in the future. This also necessitates providing adequate support materials and directly training teachers to develop and master the necessary skills to be effective educators on aspects of cybersecurity relevant to K-12 and STEM students.

It is SANS Institute's recommendation that Federal programs provide greater incentives to industry, small and medium sized organizations in industry sectors and segments, deemed critical infrastructure and key resources (CI/KR) especially that can assist with the financial challenges to start a cybersecurity education and training program until it can become engrained as a core part of company operation. This can include revisiting potential implementation of industry incentives originally intended to encourage adoption of the Cybersecurity Framework (CSF) called for in EO13636 that can be directed toward supporting the development of cybersecurity education and training programs for industry.

It is SANS Institute's recommendation that Federal programs provide greater incentives to academia to incorporate a compulsory and expanded and more relevant offering of cybersecurity education opportunities to students, especially to minorities and women that are both currently underrepresented in today's workforce of cybersecurity professionals. SANS has established our CyberTalent Immersion Academy – Women's Academy program to aid women who meet certain requirements and demonstrate aptitude and the capability to learn cybersecurity skills to build such skills and demonstrate value to prospective employers (<https://www.sans.org/cybertalent/immersionacademy/womens>). Aspects and attributes of this program could be leveraged, emulated or amplified by the Federal government.

It is SANS Institute's recommendation that Federal programs reevaluate employment practices, including employee retention and employee and veteran placement strategies to proactively assist workers with relevant cybersecurity skills to transition to the private sector in a manner that better leverages their unique skills. SANS has established our CyberTalent Immersion Academy - VetSuccess program (<https://www.sans.org/cybertalent/vetsuccess>) to aid veterans who meet certain requirements and demonstrate aptitude and the capability to learn cybersecurity skills to build such skills and demonstrate value to prospective employers. Aspects and attributes of this program could be leveraged, emulated and amplified by the Federal government.

It is SANS Institute's recommendation that the National Centers of Academic Excellence (CAE) Program, as jointly sponsored by the Department of Homeland Security (DHS) and the National Security Agency (NSA) should be closely reviewed for rigor, establish meaningful measures and public reporting of progress, results, successes and unaddressed challenges in the Program to determine its efficacy, value and return on investment.



It is SANS Institute's recommendation that the Federal Government should demonstrate leadership and define and implement a formal, sustainable workforce IT/OT cybersecurity education and training model for National infrastructure elements or organizations owned & operated by the Federal Government (e.g. TVA, Power Management Authorities, etc.) The Federal Government has the capability to immediately establish operational requirements onto these entities today, much the same as it has imposed requirements onto other Federal departments and institutions to apply the Cyber Security Framework (CSF) and Risk Management Framework (RMF).

It is SANS Institute's recommendation that the Federal Government evaluate the HM Government's Cyber Retraining Academy Programme (<https://www.cyber-academy.co.uk/retraining>). The Academy provides an intensive and immersive ten-week training programme with a mission to encourage and develop potential new cyber security professionals to enter the workforce. What makes this programme unique is it has been explicitly designed for individuals with little or no prior experience of cyber security and for those wishing to retrain and transition from other careers. Aspects and attributes of this UK programme could be leveraged, emulated or amplified by the US Federal government.

It is SANS Institute's recommendation that Federal programs find creative ways to communicate with citizens the critical importance of industry, including the exciting high-tech aspects of the systems that make, move and power the Nation and national and global economy in order to encourage the available workforce to actively seek jobs in the field, especially higher-paying jobs that require specialized skills such as cybersecurity competence.

It is SANS Institute's recommendation that Federal programs look for creative models to potentially subsidize training budgets in industries where industry associations, consortia, working groups and other similar organizations have the capability and some of their own limited budget capacity to help constituents more readily obtain cybersecurity education. Such models have shown themselves especially effective in industries comprised of many smaller entities that have limited budgets and limited staff, yet are still high-risk critical infrastructure owners and operators.

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

It is SANS Institute's recommendation that state and local governments focus on helping ensure tomorrow's workforce is gaining the necessary cybersecurity awareness and skillset to be effective as it enters the workforce. This includes seeking opportunities to expand K-12 and STEM programs to include particular focus on cybersecurity best-practices relevant to protect a citizen, but also to be applicable to industry as they enter the workforce in the future. This also necessitates providing adequate support materials and directly training teachers to develop and master the necessary skills to be effective educators on aspects of cybersecurity relevant to K-12 and STEM students.

It is SANS Institute's recommendation that state governments look for opportunities to provide greater incentives to state colleges to incorporate a compulsory and expanded, and more relevant offering of cybersecurity education opportunities to students, especially to minorities and women that are both currently underrepresented in today's workforce of cybersecurity professionals. Aspects and attributes of the SANS CyberTalent Immersion Academy – Women's Academy program of this program could be leveraged, emulated and amplified by state governments (<https://www.sans.org/cybertalent/immersionacademy/womens>).

It is SANS Institute's recommendation that state and local governments find creative ways to communicate with citizens the critical importance of industry, including the exciting high-tech aspects of the systems that make, move and power the Nation and state's economy to encourage the available



workforce to actively seek jobs in the field, especially higher-paying jobs that require specialized skills such as cybersecurity competence.

It is SANS Institute's recommendation that state and local programs look for creative models to potentially subsidize training budgets in industries where industry associations, consortia, working groups and other similar organizations have the capability and some of their own limited budget capacity to help constituents more readily obtain cybersecurity education. Such models have shown themselves especially effective in industries comprised of many smaller entities that have limited budgets and limited staff, yet are still high-risk critical infrastructure owners and operators.

It is SANS Institute's recommendation that state and local governments, similar in practice to a Federal program, seek out creative models to potentially subsidize OT oriented cybersecurity training budgets in municipal critical infrastructure systems that impart known risks to a community on a local and state level. Such models have shown themselves especially effective in other industries that are comprised of smaller entities with limited budgets and limited staff.

iii) By the private sector, including employers?

It is SANS Institute's recommendation that the private sector, employers especially recognize cyber risks are critical risks to their businesses, and incidents and attacks put not only their companies, but all who depend on the products and services they deliver at some form of risk. As such, private sector employers should adopt and maintain cybersecurity awareness, education, training and both sustainable and testable security programs into their company operations and organize their firms to ensure there is proper ownership of risks and capability to respond and recover to incidents and attacks when necessary. This includes ensuring workforce cybersecurity skills stay current and evolve with industry changes to security risks and threats over time.

It is SANS Institute's recommendation that the private sector, employers especially become proactive not reactive to invest in prevention, awareness and *good security hygiene and behaviors* as effective means to mitigate many risks and thwart many security attacks. This includes establishing cybersecurity training programs and seeking out training for employees that fit for their roles and responsibilities, and measuring *before* and *after* results of their training investments.

It is SANS Institute's recommendation that the private sector build a capability to more effectively communicate cybersecurity challenges, gaps and needs, requirements, successes, failures to a host of entities to include the Federal, state and local government as appropriate; to suppliers within their supply chain; to product manufacturers and technology providers; to service, support, maintenance and third party consulting organizations with whom they conduct business; to third party service providers and industry peers where B2B transactions are required. In all cases, the private sector's improved capability to communicate its challenges, opportunities and the like can facilitate and encourage other partners and suppliers to orient their capabilities to help address cyber risks to the private sector.

iv) By education and training providers?

It is SANS Institute's recommendation to other cybersecurity education and training providers that before any investments be made in cybersecurity education and training, in all cases, the customer's needs, objectives and expectations be carefully considered as well as a broader mission for what and how to safeguard and protect the best interests of the country, customer and company.

v) By technology providers?

It is SANS Institute's recommendation to technology providers that they adopt, implement, sustain, expand, test and challenge their own product and systems development, delivery and support processes to ensure they minimize the risks that are transferred downstream through the supply chain and to the end-users, owners and operators. This necessitates technology providers developing a disciplined process for cybersecurity risk management that both protects their own company but also all their constituents, partners and customers.

Ongoing cybersecurity education and training of technology provider personnel is an essential component, ranging from computer-based training (CBT) awareness programs to more expansive education programs that can benefit from certifying employees and enhancing career-development and hiring programs to ensure a cybersecurity-skilled workforce is available and thrives within an organization.

It is SANS Institute's recommendation to technology providers be open and forthcoming with communicating cybersecurity risks that are known or discovered in the course of business that can affect all those who interact and depend on the supplier. Coordinated disclosure practices should be followed at all times, and clear communications with partners and customers need to be second-nature recognizing that cybersecurity is always a shared responsibility. These particular skills can be learned through education and further supported by investing in workforce development and training to allow employees to build security programs that are effective and sustainable.

It is also SANS Institute's recommendation to technology providers, before any investments be made in cybersecurity education and training, that their needs, objectives and expectations be carefully considered as well as a broader mission for what and how to safeguard and protect the best interests of the country, customer and company.

Conclusion

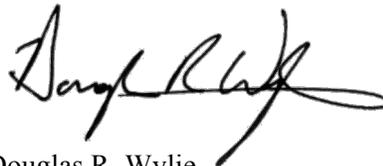
Thank you for this opportunity to respond to the NIST National Initiative for Cybersecurity Education (NICE) program RFI and for applying strong consideration to the information provided herein by SANS Institute as part of this public comment process as directed by Executive Order 13800.

Any desire by NIST and other relevant US Government agencies for further clarification with respect to SANS Institute's answers to these provided to questions can be requested at any time.

Respectfully submitted,



Michael J. Assante
Director, ICS/SCADA Security Program
SANS Institute
massante@sans.org



Douglas R. Wylie
Director, Industrials & Infrastructure Practice
SANS Institute
dwylic@sans.org