1415 N CHERRY AVE
CHICAGO, IL 60642
(312) 281-6900
UILABS.ORG
COLLABORATE@UILABS.ORG

Defining problems. Designing partnerships. Delivering solutions.

Response to NIST Request for Information: *Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development"*

UI LABS | Digital Manufacturing and Design Innovation Institute | July 2017

UI LABS is pleased to submit a response to the National Institute of Standards and Technology (NIST) Request for Information (RFI) on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development." Through our experience leading the Digital Manufacturing and Design Innovation Institute (DMDII), we are uniquely positioned to provide insight into the cybersecurity workforce development challenges facing private and public manufacturing organizations. The institute brings together universities and industry – along with startups, nonprofits, and government stakeholders – on technical and workforce development projects to accelerate the digital transformation of manufacturing. The institute engages in research and policy efforts, as well as in promoting the new digital enterprise and connected factory of the future.

Since DMDIIs inception, the institute has invested time, resources, and funding through a number of workforce development initiatives that align closely with the spirit of this RFI. The initiatives outlined below help provide context and insight to how closely our institute is working with industry, academia, and government to address the ongoing workforce needs to address cybersecurity challenges.

Assessing, Remediating and Enhancing DFARS Cybersecurity Compliance in Factory Infrastructure

DMDII requested proposals to develop a baseline understanding of costs, capabilities, and effectiveness of Department of Defense (DoD) required cybersecurity measures for factory operations, specifically those identified in DFARS 252.204-7012. This DFARS clause requires DoD contractors and subcontractors to incorporate established information security standards on their unclassified networks. DMDII requested an evaluation of the efficacy of the DFARS requirements in the face of low-end cybersecurity threats in order to ensure the protection of Controlled Unclassified Information (CUI). Leveraging the NIST cybersecurity framework the project team performed a cybersecurity assessment on 6 manufacturing companies collecting lessons learned and trending information to discern if these organizations are following the 109 requirements as outlined in NIST 800-171.

The full report provides the findings of the cybersecurity assessment and provides recommendations on cybersecurity workforce development, education and training. Should NIST or the Government like a copy of the full report, DMDII can provide it upon request. Furthermore, the methodology outlined above is an effective method of analyzing the impact of government regulations and could be applied to other compliance evaluations.

Digital Manufacturing Taxonomy

In partnership with staffing and workforce solutions firm, ManpowerGroup, DMDII has identified 165 different roles in manufacturing that will be created or transformed by the introduction of digital technology in the industry. Of the 165 roles identified, 8 are specific to cybersecurity and identify the skill sets, training, and education organizations need to invest in to ensure they are prepared for more data analytics, automation at the individual and factory level, and data connectivity throughout their organizations.

Digital Manufacturing & Design 101 Curriculum

The development of the Digital Manufacturing & Design Technology Specialization[1] was funded through a DMDII award. The University of Buffalo faculty designed the curriculum alongside industry partners, including Siemens PLM, SME, the Association for Manufacturing Technology, Moog Inc., and Buffalo Manufacturing Works. The course modules will introduce digital manufacturing and design technologies, which use data to connect and improve each stage of the manufacturing process. Of the 10-course program, Course 8 focuses solely on cybersecurity in manufacturing.

Testbed for Manufacturing Education

DMDII is in the process of developing an interactive, open cybersecurity testbed that leverages the Institute's existing 24,000 sq ft manufacturing floor which contains CNC machines, assembly stations, a metrology lab, and numerous digital technologies. The vision of the DMDII cybersecurity testbed is to demonstrate recommended cyber hygiene practices, identify and share vulnerabilities, and create a neutral environment to disseminate learnings transparently across the manufacturing community. DMDII also creates high value experiences for our partners to collaborate to develop solutions to common challenges. We have established methodologies that enables opportunities to be developed and create actionable next steps on a number of topics including cybersecurity.

The initiatives outlined above have framed DMDII's responses and recommendations to help identify what support would be needed to address the cybersecurity training, education and workforce development challenges industry, academia, and the government are currently facing. Our response is focused on cybersecurity in manufacturing, illustrating the urgency behind securing the federal supply chain network. Without additional federal support, the critical infrastructure of the U.S. supply base will continue to deteriorate, leaving the U.S. as "fast follower" and putting national security as risk.

[1] https://www.coursera.org/specializations/digital-manufacturing-design-technology

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?

Minimal data exists for cybersecurity in manufacturing education, training and workforce development efforts due to lack of cybersecurity awareness, standards and ontology, and accessibility to cybersecurity assessment tools. Until recently, when NIST published the Cybersecurity Workforce Framework, a standard for cybersecurity was abstract, leaving organizations, public and private, grappling independently with how they were going to handle their cybersecurity requirements and needs.

Currently, there is no organization or system scaling to collect data from original equipment manufacturers (OEM), small and medium manufacturers, and educational institutions around this topic to determine what areas are of most concern. The community is fragmented and is working to address the immediate threats and needs of individual organizations, but no one is looking at the community holistically and building solutions that will address the gaps in cybersecurity education, training, and workforce development in an expansive, progressive manner.

To successfully address the gaps in cybersecurity education, training and workforce development, a tool that can reach a diverse group of organizations at scale is critical to sourcing and analyzing cybersecurity needs. Leveraging existing tools and networks, such as DMDII's Digital Manufacturing Commons (DMC) in partnership with NIST's Manufacturing Extension Partnership (MEP) network, would be invaluable when working to collect data, address critical cybersecurity elements and drive to make a measurable impact across a diverse community.

The DMC, a secure, open source multi-party collaboration platform, is a viable method to reach the diverse ecosystem. With the appropriate resources allocated to such a project, the DMC could introduce a training and certification program in cyber hygiene in the manufacturing environment, provide organizations with access to the latest technologies and mitigation techniques to secure legacy manufacturing systems and continually refresh their skills, and accelerate SMMs ability to meet their workforce needs and achieve best practices for cybersecurity.

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

The cybersecurity workforce is not keeping pace with the increasing demand of information technology requirements, or the roles that fill them. The manufacturing sector is increasingly digitally driven, a trend that opens 12%, or $2 trillion, of the U.S. GDP[2] to the possibility of cyber-attack – and the more successful the U.S. becomes at digitization, the more inviting these attacks become. Both employers and workforce can benefit from a focus on what skills and future expertise is required to detect and protect against these threats.

[2] World Bank Development Indicators, 2015

The macro challenges around manufacturing workforce shortages are widely known; what might not be so well-known is what the digital skill areas and digital related roles are, where the target digital workforce sources are, and when to invest in those skills and roles. For example, employers are often unsure or unaware of the types of skills needed to implement digital technologies required to achieve a secure manufacturing floor. Employers struggle connecting their manufacturing systems to business side-data systems, and what the utility of these skills yields for their business versus the skills required on a manufacturing floor even a decade ago. As we work to close a skills and labor gap in manufacturing, we cannot forget to look to the cybersecurity skills our workforce need to thrive in the next and future manufacturing environments.

In partnership with ManPower, DMDII published a Digital Manufacturing Taxonomy. This research is a starting point to define who digital manufacturing and design workers are, what their work looks like, and how it contributes to the overall organization. Our research identified a broad set of 165 potential roles and role descriptors in digital manufacturing and design and 20 success profiles for representative roles. These roles are only a portion of the ones we believe will provide the bridge between our current and future workforce. With the full picture of the broad community of roles and technical domain structures, we see an aligned and accelerated path for digital manufacturing workforce development and economic benefits for individuals and companies alike. Of the 165 roles identified, 8 cybersecurity roles were documented in our research. A cybersecurity taxonomy would benefit industry, academia, and government to help organizations make informed, educated decisions on which cybersecurity role is the best suited to address their unique needs. Without such a structure, organizations are independently identifying needs without seeing the full picture.

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?

Many of DMDII's academic members are investing their efforts heavily in cybersecurity workforce development programs. Within our consortia, 19 organizations, spanning 16 states have invested in 29 cybersecurity workforce development programs through the National Science Foundation CyberCorps program. The programs being established span from developing a set of building blocks and methodologies for designing virtual industrial control system test beds to cybersecurity teaching in high school environments utilizing virtual reality three-dimension games, robotic programming games, practical ethical hacking labs, and cyber forensics labs based on simulated cases. With an existing programming investment of $56,785,729 amongst our partners, DMDII is well positioned to leverage the existing curriculum, methodologies and frameworks to effectively scale and disseminate the program practices and learnings.

Many of the programs referenced above, are focusing on immersive learning environments. Based on a recent study[3], the most effective way to educate students in STEM is through hands-on learning environments rather than standard lecture settings. The study found that undergraduate students in classes with traditional stand-and-deliver lectures are 1.5 times more likely to fail than students in classes using more stimulating, so-called active learning methods.

DMDII has purposely pursued building a hands-on digital manufacturing learning environment to train students, employees and executives on our manufacturing floor. We've developed a neutral space for experimentation and development of next generation digital manufacturing solutions called the Future Factory Platform.

Many of our top tier partners believe the use of the Future Factory Platform is a critical element in cybersecurity workforce education and training. One partner expressed their confidence in this initiative sharing, "We are supportive of using the DMDII Future Factory as a manufacturing cyber security testing and training facility and we like the emphasis on best practices, including the ability to engage participants from numerous communities (both public and private) in a hands on, working production environment." Another partner who is a globally leading software provider in our network is especially enthusiastic about the development of the testbed stating, "Reading a book about cybersecurity does not prepare you to defend your manufacturing data. This is a complex topic with lots of moving parts (methods, tools, protocols, threat models, etc.). Having a hands-on learning environment where students can learn the latest on tools and best practices, and experiment with the next generation of cybersecurity tools is essential to the success of digital manufacturing."

DMDII is willing and able to activate this space for cybersecurity education, training and workforce development in the following capacities:

1. Develop secure and trusted mechanisms for management of manufacturing data, including systematic methods for detection, measurement and metrics, statistical tests, and attack models to study the physical effects of machine behavior during cyber-attacks.
2. Facilitate coordination of R&D across organizations in the area of cybersecurity in manufacturing. DMDII will push innovations in cybersecurity architecture for control systems and network configuration compliance, while providing an R&D testbed to facilitate assessment of cybersecurity product design and execution.
3. Fill the need for an operating partner in execution and communication of cybersecurity standards and frameworks, and will accelerate secure digitization of the supply network through cutting edge technology development on machine-machine (M2M), machine-cloud (M2C), and machine-human (M2H) cybersecurity protocols and standards. DMDII will engage standards development organizations, such as the National Institute of Standards and Technology (NIST), the International Society of Automation (ISA) and the International Electro-Technical Commission (IEC), to further develop and refine guidelines and standards facilitating the implementation of non-invasive cybersecurity requirements in advanced

[3] Freeman S, Eddy SL, McDonough M, Smith MK, Okoroafor N, Jordt H, et al. Active learning increases student performance in science, engineering, and mathematics. PNAS. 2014;111(23):8410–5.

manufacturing and industrial control systems. The resulting methods and technologies will benefit both original equipment manufacturers (OEMs) and SMMs who will be able to leverage cyber frameworks created and demonstrated by DMDII.

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

In early July DMDII held a cybersecurity workshop with a diverse set of partners from industry, academia and government with the objective to build a multi-year cybersecurity roadmap for the DMDII testbed, outlined above, that will address the challenges they face within cybersecurity. Through a set of interactive sessions two themes emerged, that if addressed, could create a major impact within the ecosystem.

1. **Cybersecurity Risk Assessment for Manufacturers**: While the Government and industry have focused much of their efforts on protecting technical information in business and engineering information systems, less attention has been paid to enhancing protections for OT systems, which enable the flow of technical data in factory floor networks and industrial control systems. Department of Homeland Security (DHS) investigations of cyber-attacks on the U.S. manufacturing sector in 2015 had doubled when compared with the previous year.[4] Defense contractors throughout DoD's supply chain have been targets of cyber-crime – a growing threat that has a direct impact on national security. As a direct result, DoD issued new contract clauses with mandatory flow down to subcontractors requiring established information security standards and reporting of cyber intrusion incidents. The nation's SMMs, which comprise 80% of all manufacturers, are struggling mightily to comply. The SMM community needs tools, resources and additional education to ensure our supply chain is secure from cyber-threats.

   A recently funded DMDII project highlights the struggles SMMs are having with cybersecurity DFARs compliance. The study found that not a single requirement of the 109 outlined in NIST 800-171 was compliant across all organizations and only 1 requirement was compliant in 80% of the companies.

Requirement Compliance Counts				
Company	Compliant	Partial	Non-Compliant	N/A
Company E	20	69	20	0
Company D	10	51	44	4
Company C	19	73	17	0
Company B	9	75	25	0
Company A	7	56	46	0
Company 0	14	40	54	1
Average	**13.2**	**60.7**	**34.3**	**1.3**

[4] "Cyber-attacks against US critical manufacturing have nearly doubled – DHS", RT Question More, January 15, 2016

These results are staggering and highlights how immediate the need is to reach this community and provide them with education and resources to secure their organizations. Improving the cybersecurity posture of individuals and organizations by disseminating curriculum, frameworks and possible solutions is the beginning of risk mitigation across the national supply base.

2. Cybersecurity SMM Adoption: Cybersecurity for manufacturing is a non-value add component to manufacturing – cybersecurity does not increase profits but rather reduces risk. Therefore, cybersecurity is beyond the investment risk of many SMMs. Without a concerted effort to assist SMMs with the right solutions, the adoption of cybersecurity standards, and the efficiencies of an open source manufacturing platform, meaningful impact in cybersecurity awareness across the entire value chain may not be realized for years to come.

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)?

Advancement in technology has led to an unprecedented exposure within manufacturing facilities. As the number of interconnected devices continues to increase, so does the amount of access points for cyber-attacks. As a result, effective cyber training is a necessity to prepare the workforce for organizational needs. Unfortunately, educators face significant challenges trying to keep pace with the technology advances to ensure they are providing current, relevant curriculum and training.

A study released in July of 2016 by Intel Security with the Center for Strategic and International Studies (CSIS) takes a closer look at the cybersecurity workforce shortage across eight countries including Australia, France, Germany, Israel, Japan, Mexico, the U.K., and the U.S. The report found that only 23% of respondents believe education programs are actually preparing students to enter cybersecurity work.[5] With this glaring response it’s clear education methods need to transform in order to have confidence in workforce preparedness.

Without a focus on addressing the skills shortage in cybersecurity, the U.S. manufacturing base is at high risk. The shortage in cybersecurity skills does direct and measurable damage, according to 71% of IT decision makers who are involved in cybersecurity within their organization. One in three say a shortage of skills makes their organizations more desirable hacking targets. One in four say insufficient cybersecurity staff strength has damaged their organization’s reputation and led directly to the loss of proprietary data through cyberattack.[6]

[5] “Hacking the Skills Shortage”, intel Security, July 2016

[6] “Hacking the Skills Shortage”, intel Security, July 2016

Curriculum development needs to evolve and become agile, to react quickly to industry needs based on innovation and tech disruption. As industries transform, curriculum needs to align and provide education on standards, technologies and best practices to facilitate student and organizational success. With the appropriate support of the government and our partners, DMDII can facilitate progress in educating our workforce through cybersecurity curriculum development and hands-on learning through our testbed.

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?

Continued funding at the federal level is a critical element in keeping the U.S. manufacturing sector globally competitive and secure. Without support from the federal government the sectors across the U.S. will work to address cybersecurity concerns in silos, reinforcing the fragmented solutions.

It is imperative that the Government continues to support private and public partnership to fund cybersecurity and workforce initiatives at the federal level. In doing so, the government gets exposure to innovation and can provide better public services through improved operational efficiency. Additionally, in some cases, the Government is able to double their investments by leveraging private funding through cost share efforts.

DMDII is well positioned to support the government in curating impactful public-private partnerships. Leveraging our cybersecurity testbed and our network DMDII is able to demonstrate and disseminate learnings on recommended cyber hygiene practices and vulnerabilities. Using the Digital Manufacturing Commons and our partnership with Illinois Manufacturing Excellence Center, DMDII can provide the Government a broad, expansive reach across the U.S. to reach the organizations within the manufacturing community that are at the highest risk of cyber-attacks.

Providing funding through organizations that bring diverse set of stakeholders together, such as DMDII, the U.S. will begin to address complex problems, such as cybersecurity workforce skills gap, that individual organizations cannot solve on their own.

Thank you for the opportunity to contribute to strengthening the U.S. cybersecurity workforce in manufacturing. We truly believe in this mission and feel strongly that we can make an impactful difference to securing the U.S. supply base.

We thank you for taking the time to consider our views. Should clarification be required or more information needed, please reach out to Kristen Preble at, kristen.preble@uilabs.org or (312) 281 – 6869.

Very best regards,

Caralynn Nowinski Collens
Chief Executive Officer, UI LABS
caralynn.collens@uilabs.org
312-281-6820

Thomas McDermott
Executive Director, DMDII
Thomas.mcdermott@uilabs.org
312-281-6854