REQUEST FOR INFORMATION
Executive Order on America's Cybersecurity Workforce

Cyber-physical Systems Workforce Status

This Request for Information (RFI) is issued by the Washington Headquarters Services Acquisition Directorate (WHS/AD). This RFI seeks Government agency and industry comments to assist the Government in identifying cybersecurity workforce gaps and training requirements for cyber-physical systems (CPS). This RFI is not a request for a capabilities statement, rather a reporting of the status (skills required, known gaps and related curricula) of the CPS workforce.

Respondents are asked to answer the questions below or complete the attached spreadsheet which is more detailed and provides a level of granularity more useful for analysis and recommendations for government action. Additionally, Respondents are invited to join a CPS Workforce Focus Group that will meet weekly August through September 2019 (dates and times to be determined) to gather and analyze the information required. Respondents may take part in the focus group by responding to the attached inquiry or by active participation in the focus group meetings. Responses may be sent to the POC at the bottom of this RFI.

Objective

The US Department of Defense (DoD) is requesting information to assist the Government in identifying and evaluating skill gaps in Federal and non-Federal cybersecurity personnel and training gaps for specific critical infrastructure sectors, defense critical infrastructure, and the Department of Defense's platform information technologies; and recommending curricula for closing the identified skills gaps for Federal personnel and steps the United States Government can take to close such gaps for non-Federal personnel by, for example, supporting the development of similar curricula by education or training providers.

The Executive Order (EO) on America's Cybersecurity Workforce calls for a report to the President "To strengthen the ability of the Nation to identify and mitigate cybersecurity vulnerabilities in critical infrastructure and defense systems, particularly *cyber-physical systems* (CPS) for which safety and reliability depend on secure control systems…"

Cyber-physical systems: Legacy and smart systems that include engineered isolated or interacting networks of physical and computational components (also known as control systems, industrial control systems, SCADA, DoD weapon systems and non-traditional information technology systems in utilities, logistics, manufacturing, nuclear, chemical, biological, processes, etc.). CPS and related systems (including the Internet of Things (IoT) and the Industrial Internet) are widely recognized as having great potential to enable innovative applications and impact multiple economic sectors in the worldwide economy (https://www.nist.gov/el/cyber-physical-systems).

REQUEST FOR INFORMATION
Executive Order on America's Cybersecurity Workforce

Cyber-physical Systems Workforce Status

Specific Questions for Government and Industry

Specifically, for each of the following Competency Areas, request useful descriptions of 1) existing skill gaps of the CPS workforce in the Respondent's organization, and 2) the underlying cause of the skill gaps (e.g., personnel shortfall, lack of training or training curricula) and 3) recommendations to address each gap.

Competency Areas:

1/ Management or governance of CPS cybersecurity including familiarity with all CPS sub-systems and components, configuration management, cybersecurity and RMF assessment and authorization of CPS, establishment of security policies and procedures, familiarity with governance (e.g., policy, ownership, vendor arrangements), and the ability to establish procedures for continuous monitoring, new vulnerabilities and response to alerts.

2/ Performance of CPS cybersecurity, such as continuous monitoring, knowledge of normal operations of cyber-physical electrical and mechanical systems, and when (and to whom) to report abnormal operations.

3/ Technical ability to manage corrective, preventive, and predictive maintenance, including application of cybersecurity patches, specification of cybersecurity requirements, and applying protections for on-going vulnerabilities and newly discovered threats.

4/ Knowledge of Energy and/or Water CPS, associated cybersecurity requirements for Utility Energy Service Contract (UESC) and Energy Savings Performance Contracting (ESPC) projects, including ensuring competing regulations and maintenance procedures to not create vulnerabilities in CPS.

5/ Ability to ensure cybersecurity requirements are established and standard operating procedures are in place for the safe operation of cyber-physical systems.

6/ Knowledge and ability to "design in" and specify cybersecurity requirements during design of cyber-physical systems and associated architectures.

7/ Knowledge and understanding of potential cybersecurity vulnerabilities in technology that integrates and optimizes "high-performance building / facility" attributes, including energy efficiency, durability, life-cycle performance, and occupant productivity.

8/ Cybersecurity management of critical systems, including identifying connections to critical physical systems, ensure training and compliance for personnel that support the assets and operations associated with critical systems, testing and evaluation of the effectiveness of information security

policies, procedures, practices, and security controls, remedial actions, and incident detection, reporting and response, execution of continuity of operations.

9/ Business, budgetary and contracting skills to identify and assess evolving cybersecurity risks and requirements to ensure delivered products support critical missions.

Additional Questions for Government and Industry

10/ What additional cybersecurity skill gaps for CPS exist in the Federal or non-Federal workforce? Please describe with enough detail for analysis.

11/ Does appropriate budget exist to cover necessary training identified? If yes, provide approximate annual budget. If not, provide estimated shortfall per FY.

12/ Does appropriate budget exist to secure CPS? If yes, provide approximate annual budget. If not, list estimated shortfall per FY.

13/ Please provide the total number of positions to which a particular competency applies within your environment.

14/ Please provide the total number of Cyber-physical positions within your footprint.

15/ Please provide any additional comments in support of this RFI.

RFI Guidelines

Please note that this synopsis is for INFORMATION and PLANNING purposes only and does not constitute a Request for Quote (RFQ). Responses to the RFI cannot be accepted by the Government to form a binding contract nor will the Government pay for the information solicited or recognize any costs associated with the submission of the RFI. The purpose of the RFI is to provide an opportunity for industry to enhance the success of any future procurement. Any information obtained as a result of this RFI is intended to be used by the Government on a non-attribution basis for program planning and acquisition strategy development. Providing data/information that is limited or restricted for use by the Government for that purpose would be of very little value and such restricted/limited data/information is not solicited. By submitting information in response to this RFI, submitters of such information impliedly consent to the release and dissemination of submitted information to any Government or non-Government entity to which WHS releases and disseminate the information for review. As such, to the extent that any information submitted in response to this RFI is marked as or construed to be proprietary or business- sensitive, submitters are hereby notified (a) about the potentiality that such information may be disclosed to third parties and (b) that submission of

information in response to this RFI constitutes consent to such handling and disclosure of submitted information. Responses to this notice are not considered offers and cannot be accepted by the Government to form a binding contract.

Submission Requirements

Respondents are invited to submit a response to the questions as stated above or via the Excel spreadsheet to the "RFI: Cyber-physical Systems Workforce Status." All responses should be submitted via e-mail to Daryl Haegley at daryl.r.haegley.civ@mail.mil no later than 5:00 PM (EST) on September 13, 2019. Only attach MS Word/Excel compatible files or Adobe Acrobat PDF files in electronic correspondence. Telephonic inquiries will not be considered. Please provide response POC information and CPS Focus Group participant contact information, if applicable.

Following virtual meetings will provide

CPS Work Force WG virtual mtg links below; dial: Number: 844-531-0958 Participant Code: 927698915

#1
07 Aug 3pm EST https://conference.apps.mil/webconf/kpkebcisp9bru87q9qix68bbnaascany

#2
14 Aug 10am EST https://conference.apps.mil/webconf/bo05xm9k2y9rhgi92vcmx2glq9bdr3u1

#3
21 Aug 2pm EST https://conference.apps.mil/webconf/i8yredrjxc6vy5069k0qau4rwbubjdo4

#4
04 Sept 10am EST https://conference.apps.mil/webconf/0swnehf75z11l5q5b1z292nwe097viir

#5
11 Sept 2pm EST https://conference.apps.mil/webconf/73hzdh5m5zv47nzhgv8x99q2pnj485kn