REQUEST FOR INFORMATION

Office of the Under Secretary of Defense (OUSD) Research and Engineering (R&E) Cyber Science and Technology (S&T) Roadmap

July 23, 2020

1.0 NOTICE TYPE:
Pre-solicitation

Notice ID: RFI-WHS-20-CYBERST

2.0 SYNOPSIS:
This is a Request for Information (RFI) only. This RFI is issued solely for information and planning purposes – it does not constitute a Request for Proposal (RFP) or a promise to issue an RFP in the future. This request for information does not commit the Government to contract for any supply or service whatsoever. Furthermore, the OUSD (R&E) is not at this time seeking proposals and will not accept unsolicited proposals. Responders are advised that the U.S. Government will not pay for any information or administrative costs incurred in response to this RFI. All costs associated with responding to this RFI will be solely at the interested party's expense. Not responding to this RFI does not preclude participation in any future RFP, if any is issued. If a solicitation is released, it will be synopsized on the Beta SAM website (https://beta.sam.gov/). It is the responsibility of the potential offerors to monitor these sites for additional information pertaining to this requirement.

3.0 DESCRIPTION

The National Defense Authorization Act (NDAA) for fiscal year 2020, section 257 (§257), directs the Secretary of Defense, acting through the Under Secretary of Defense for Research and Engineering USD (R&E), to develop a roadmap S&T activities of the Department of Defense (DoD) to support the development of cyber capabilities to meet Department needs and missions.

The Department's S&T Program invests in and develops capabilities that advance the technical superiority of the U.S. military to counter new and emerging threats. The USD (R&E) established an Assistant Director (AD) for Cyber who is the modernization lead responsible for unifying and advancing the Department's cyber investments and capabilities. The AD is seeking information from interested contractors, academia, and Federally Funded Research and Development Corporations (FFRDCs) in support of the development of a Cyber S&T Roadmap for capabilities ready for operational use within the next 25 years or earlier.

4.0 BACKGROUND

USD (R&E) serves as the Department's chief steward and advocate for unifying and advancing the Department's investments and capabilities aligned with the National Defense Strategy's modernization priorities. A key modernization priority area is cyber. The 2018 DoD Cyber Strategy (DCS) articulates how the Department will implement the priorities of the National Defense Strategy in and through cyberspace.

The DCS calls for "increased investments to accelerate the development and rapid transition of technologies that provide the basis for 1) vastly enhanced resilience of DoD systems and critical infrastructure 2) substantially increased capacity and unrivaled capabilities for the conduct of cyber

and cyber-enabled operations, 3) overmatching skills and expertise within the Cyber Mission Forces, and the Cybersecurity and Cyber S&T workforces…."[1]

The Department's cyberspace objectives articulated in the *2018 DoD Cyber Strategy Summary* are:
"1. Ensuring the Joint Force can achieve its missions in a contested cyberspace environment;
2. Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages;
3. Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident;
4. Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and
5. Expanding DoD cyber cooperation with interagency, industry, and international partners."

The Department's S&T Program invests in and develops capabilities that advance the technical superiority of the U.S. military to counter new and emerging threats. The USD (R&E) established an Assistant Director (AD) for Cyber, who is the modernization lead responsible for unifying and advancing the Department's investments and capabilities for Cyber. In this role, the AD's responsibilities include:

- Establishing a DoD-wide, mission-focused roadmap to chart the path to deliver the cyber technical capabilities needed by our warfighters
- Assessing the range of cyber activities in their technical area, including what is occurring in DoD, other executive branch agencies, the commercial world, academia, and other countries
- Leading independent technical analyses
- Conducting engagement and outreach across the community

The AD for Cyber, Dr. Daniel Ragsdale, is responsible for the development of the "Road to Dominance Strategy and has been designated to lead the effort to develop the Department's response to NDAA 2020 §257. DoD has also formed S&T Communities of Interest (COI)s. Each COI coordinates investments by DoD Services and Agencies in applied research and advanced technology development in the relevant area, develops a DoD-wide S&T Roadmap in that area, facilitates leverage across the DoD and facilitates interactions with Industry, Federally Funded Research & Development Center (FFRDC), other Government Agencies and academia. Cyber is one of the COIs established by the DOD.

NDAA 2020 §257 directs the Secretary of Defense (SECDEF), acting through the Under Secretary of Defense (USD) for Research and Engineering, to develop a roadmap for science and technology activities of the Department of Defense to support the development of cyber capabilities to meet Department needs and missions. The roadmap must ensure consistency with Federal interagency, industry, and academic activities.

The technical scope of the roadmap covers the development of cyber operations and cybersecurity capabilities. The time horizon for these cyber capabilities is for operational use within the next 25 years or earlier. The Government is focusing on 2020-2025; 2025-2030; and beyond 2030. This roadmap will be developed in an unclassified form but will include a classified annex. The SECDEF shall make available to the public the unclassified form of the roadmap developed.

Security Clearance: No security clearance is required to respond to this RFI.

---

[1] https://www.congress.gov/116/meeting/house/110655/witnesses/HHRG-116-AS26-Wstate-GriffinM-20200311.pdf

5.0 REQUESTED INFORMATION

Innovation is vital to our national economic success and technological advantage. “Cyber is a unique operational domain with significant security challenges and potential leap-ahead capabilities for military operations requiring enhanced command, control and situational awareness, and autonomous operations. Ability to gain and maintain the U.S. technological edge in cyberspace in the face of rapid evolution is essential to maintaining mission readiness.[2] Our future economic strength requires a significant increase in cyber research and development and greater collaboration among government, industry and universities. Consequently, trends, visions, and ongoing and planned S&T contributions from other government agencies, industry, FFRDCs, and academia will be very valuable inputs to develop the roadmap.

This RFI is an opportunity for all interested parties to share their R&D projections, technical capabilities, and demonstrated experiences in cybersecurity and cyberspace operations. To gain the most value from this request, the Government is providing information to potential responders on the goals of this study and the requested time horizons. All interested responders are invited to provide written response to the requested information below.

Responding to this RFI will assist OUSD (R&E) in determining the potential levels of research and technical capability within industry to support the S&T roadmap. The Government is most interested in cybersecurity and cyber operations technologies that will affect cyber S&T investments in the 2025-2030 timeframe (mid-term future), but your organization’s input for the other two time periods is also very valuable. The OUSD (R&E) requests that organizations identify a primary Point of Contact (POC) to provide their organization’s inputs in white paper format.

The requested inputs include, but are not limited to your organization’s:

- Cyber vision and program goals
- Capability areas and expertise, as they apply to the following system types:
    - National security systems
    - Weapon systems
    - Business systems
    - Critical infrastructure systems
    - Enterprise and network systems
- Cyber facilities and testbeds
- Research priorities
- Current and future (projected) internal and external cyber program activities and plans
- Major prototyping and demonstration programs
- List of agreements and activities to transition capabilities into acquisition activities, commercial use, or production,
- Cooperative activities with international partners,
- Efforts under the Small Business Innovation Research and the Small Business Technology Transfer Program,
- Partnerships between the DoD and your organization (e.g., universities participating in National Centers of Academic Excellence in Cyber Operations and Cyber Defense).

Specific questions to be addressed are provided in the attachment. Given the broad technical and operational considerations of the Department and the research scope spanning basic research, applied research, development, and facilities and equipment, interested parties are not obligated to respond to

---

[2] *https://www.cto.mil/modernization-priorities/*

every question. Instead they may respond to questions pertinent to an organization's technical focus, expertise and research type.

6.0. RESPONSE SUBMISSION FORMAT

Interested parties are requested to respond to this RFI with a capability whitepaper. The RFI whitepaper should be in Microsoft Word for Office 2007 compatible format and is **due NLT 21 August 2020, 1700 EDT**. Submissions shall be formatted for printing on 8-1/2 by 11inch paper with font size not smaller than 12 point in Microsoft Word or Adobe PDF format with at least one-inch margins. Font sizes of 8 point may be used for figures, tables, and charts. Late responses will not be considered.

Each unclassified white paper shall consist of the following sections:

Section 1: Cover Page (1 page)

- Organization
- Technical point of contact (name, title, address, phone number, and email address)
- Administrative point of contact (name, address, phone and fax number, and email address)

Section 2: Section 2 of the white paper shall provide the information requested in Section 3 of this RFI and responses to the questions provided in the attachment. The whitepaper responses shall be limited to 15 single-sided pages for section 2 and shall be submitted via e-mail only to the Government Point of Contract (POC).

The Government Point of Contact (POC) for the evaluation of the RFI whitepaper is: chester.j.maciag.civ@mail.mil. **Please no phone calls**.

Given the broad technical and operational considerations of the Department and the research scope spanning basic research, applied research, development, and facilities and equipment, interested parties are not obligated to respond to every question. Instead they may respond to questions pertinent to an organization's technical focus, expertise and research type.

Schedule of Events		
Event	**Date**	**Time**
Questions Regarding RFI	7 August 2020	1700 EDT
RFI Responses Due	21 August 2020	1700 EDT

The Office of the Under Secretary of Defense for Research and Engineering does not plan to respond to submissions other than to confirm receipt. OUSD (R&E) will review all inputs for consideration when developing the S&T roadmap and technology projections. In some cases, OUSD (R&E) may request additional information and/or facilitate exchanges on a particular area of technology.

7.0 INDUSTRY DISCUSSIONS

The Government representatives may or may not choose to meet with potential responders. Such discussions would only be intended to get further clarification of potential cyber capabilities.

8.0 QUESTIONS

Questions on the whitepaper regarding this RFI should be submitted in writing by e-mail to Chester J. Maciag, Director for Cyber Technologies, chester.j.maciag.civ@mail.mil with subject line reading "Cyber RFI Question." Verbal questions will not be accepted.

9.0 SUMMARY

This is a request for information (RFI) only to identify sources that can provide Cyber S&T roadmap activities and projections. The information provided in the RFI is subject to change and is not binding on the Government. OUSD (R&E) has not made a commitment to procure any of the items discussed, and the release of this RFI should not be construed as such a commitment or as authorization to incur cost for which reimbursement would be required or sought. All submissions become Government property and will not be returned.

ACTIVE

Contract Opportunity

Notice ID

RFI-WHS-20-S&T

Related Notice

Department/Ind. Agency

DEPT OF DEFENSE

Sub-tier

The OFFICE UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING (OUSD/R&E)

Office

DEPUTY DIRECTOR RESEARCH & ENGINEERING, ASSISTANT DIRECTOR CYBER (DDR&E/AD/CYBER)