UNCLASSIFIED

REQUEST FOR INFORMATION RESPONSE

ESTABLISHING A GOVERNMENT EFFECTIVENESS ADVANCED RESEARCH (GEAR) CENTER

SUBMITTED BY

X Corp Solutions, Inc. 1000 Corporate Drive #119 Stafford, Virginia 22554	Cesar Nader, President and CEO Phone: 540-847-0671 Email: cesar@xcorpsolutions.com
DUNS Number: 967917704	CAGE Code: 6C9K7
Business Type: SBA 8(a) Small Disadvantaged Business (SDB), Service Disabled Veteran Owned Small Business (SDVOSB)	
NAICS Codes: 541990, All Other Professional Scientific, and Technical Services; 541330; 541513; 541611; 541618; 541690; 541930; 541990; 561210; 561612; 611710	
Active facility security clearance level: Top Secret	

Cesar@xcorpsolutions.com
Telephone: 540-847-0671
www.xcorpsolutions.com

X Corp Solutions, Inc. (XCorp) is an 8(a) Small Disadvantaged Business (SDB) and verified Service Disabled Veteran Owned Small Business (SDVOSB), that is building a Cyber Security Center of Excellence (CSCE) with many of the core competencies envisioned for a GEAR Center. We are collaborating with government, academia, and industry relative to the knowledge, skills, and abilities needed for the cyber workforce to include ensuring that they are qualified and proficient. XCorp holds a Top Secret Facility Clearance and we are ISO 27000 and ISO 9001-2015 certified.

Sincerely,

Cesar E. Nader
President and Chief Executive Officer (CEO)
X Corp Solutions, Inc.

Due Date: September 14, 2018

Executive Summary

X Corp Solutions, Inc. (XCorp) is building Phase I of the Government Effectiveness Advanced Research (GEAR) Center. In April 2018, XCorp broke ground for a 30,000 ft^2 facility located at Quantico Corporate Center (QCC) in Stafford, Virginia. The Cyber Security Center of Excellence (CSCE) is focused on delivering and sustaining a qualified workforce to the Cyber Security Community of Practice. The CSCE is based on the same founding principles articulated in the RFI for a GEAR Center as well as the essential elements of collaboration among government, academia, and industry.

The managing entity of the CSCE is a non-profit organization and its members form a consortium representing all aspects of cyber security. Proximity to Marine Corps Base Quantico enables collaboration with tenant activities aboard the base such as the Department of Defense (DoD) and Department of Justice (DoJ) as well as local and state agencies.

Within the context of cyber workforce professionalization and "upskilling or reskilling," CSCE consortium members have collaborated with Headquarters Marine Corps, Marine Corps Training and Education Command, the Virginia Community College System, Universities in Virginia, and the Commonwealth of Virginia regarding professionalization strategies for Future Force 2025 and training veterans in cyber. Industry partners in that effort include Microsoft, Cisco, Amazon Web Services (AWS), (ISC)^2, and Fortinet. These skills are essentially and fundamentally agnostic to the organization and delivery of the constantly changing content, requiring a non-traditional approach not typical in academia. The CSCE consortium has the capability to deliver new content synchronously to the enterprise from an instructor located anywhere. This is a critical element of upskilling and/or reskilling any workforce.

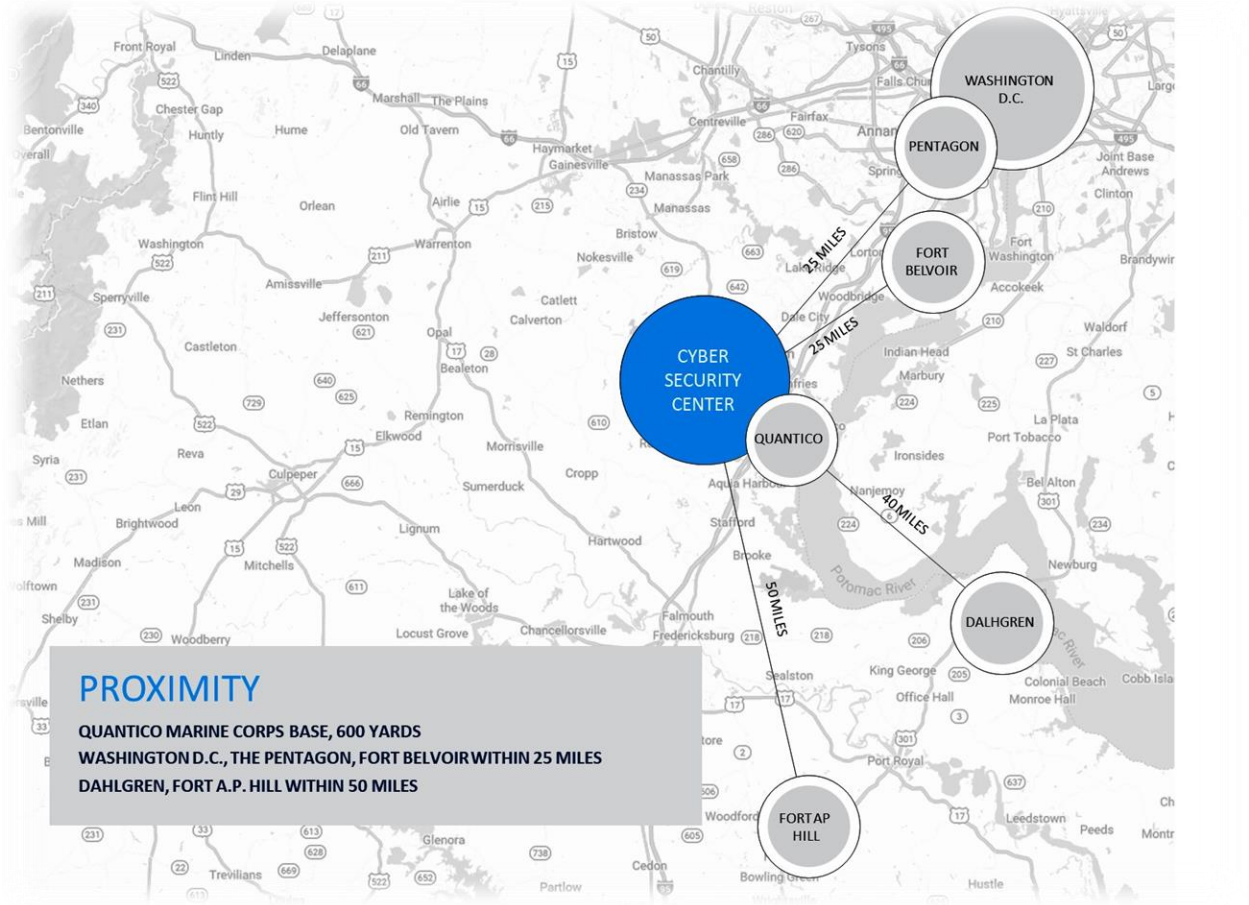
Responses to RFI Questions

Informing the GEAR Center

1.0 Given the mission of the GEAR Center, what should be:

1.1 Its strategic approach and operating objectives?

The strategic approach for the GEAR Center should be inclusive of: local, state, and federal government; community colleges and universities (public and private); national laboratories and research centers; and, private industry. Outreach to these entities for collaborative relationships will be essential for the GEAR Center to be innovative and, more importantly, aware of trends in technology and the learning sciences. The pace of technology development requires that education and training for the reskilling and upskilling of the workforce be considered concurrent with technology development to deliver capability within operational context. The location of the Cyber Security Center of Excellence (CSCE) represents the "proximity" necessary to enable routine collaboration among all stakeholders.



The GEAR Center should focus on developing and promoting initiatives that enhance the operational efficiency and capabilities of the agencies of federal, state and local government. In support of state and local government, a focus on "Smart Cities" in the following areas: Transportation; Utilities; Public Safety; and, Citizen Services. The Gear Center should:

- Support the identification of areas where technology innovations are potentially transformative;
- Provide general and specific guidance on migration strategies and assistance to government entities in their migration efforts;
- Facilitate education and training reskilling and upskilling programs that target proficiencies needed to support emerging areas of technology deployment
- Provide support for focused new IP creation and innovation that would be transformative, including commercial translation and business incubation in areas of focus;
- Facilitate grant and shared investment funding for emerging technologies and pilot/demonstration projects.

1.2 Specific areas of innovation and practice to prioritize?

"Cyber" is probably the most important and challenging area that requires innovation in methodologies of education, training, and qualifying the workforce. "Cyber" is cross as well as multi-disciplinary and touches every aspect of our lives. Upskilling and reskilling is necessary for both the community of practice as well as for those who deliver the content. Effective and efficient delivery of curated content by those who are most qualified to determine proficiency will be an ongoing challenge faced by all "formal" stakeholders within that community of practice. The CSCE consortium has a methodology for curation of content and is on the leading edge of learning science design with a cognition design laboratory affiliated with George Mason University and the Serious Game Institute.

Working with academic and industry partners, the GEAR Center should prioritize the comprehensive understanding of technology trends and development of a recommended "reference model" describing how federal, state and local governments would consider in planning their respective migration from existing legacy systems and services to 21st Century, technology enabled ones. The Center should motivate and support the sharing of data and solutions between and among the various stakeholders, encouraging state and local governments to contribute their data to complement federal data sources. Establishing a data and analytics "federation" will provide near-term and long-term benefits as data collection and ingestion capabilities continue to improve and IoT and related "edge" device technologies begin to contribute massive quantities of new data. Importantly, any and all such data sharing will enhance the ability to apply machine learning and AI solutions in the development of solutions.

1.3 The process to identify and prioritize additional new areas on an ongoing basis?

Recommendation is that the GEAR Center establish a governing/advisory board comprised of representation from the various stakeholders to provide oversight, guidance and prioritization. The CSCE has implemented this strategy with both a Board of Directors and an Advisory Board. The board should include sub-committees that have focus in sub-areas such as training, innovation, etc. to ensure that the Center has a balanced and informed understanding of high-level strategic direction as well as the technical insights that should guide tactical and operational initiatives.

2.0 How should a GEAR Center be operationalized, including its structure, such as a physical center, a network, a consortium of institutions, or other approaches?

The methodology of operationalizing the CSCE is appropriate for the GEAR Center. The CSCE would be the facility that houses the activities of the GEAR Center and it is "connected" via proximity and access to significant bandwidth. This "on net" connectivity allows for virtual participation with research institutions worldwide via the Open Research Cloud Alliance (ORCA). The operations and maintenance of the CSCE is accomplished by a non-profit organization that also manages the consortium. In this instance, the non-profit organization is the Cyber Bytes Foundation (CBF) and the CBF is oriented to the cyber security community of practice. However, the operationalization of the CSCE can scale laterally to other disciplines of interest and/or demand by the GEAR Center.

3.0 What models of public-private partnership should inform the GEAR Center?

The GEAR Center faces new types of challenges that require new and innovative thinking. Emerging technologies and capabilities have blurred the lines between those things that can/should be delivered through government agencies and those that can be consumed as commercial services. The pace of innovation in industry and academia and aggressive disruptive technology deployments by emerging start-up companies both compound this challenge and present unprecedented opportunities. As a result, the sort of public-private partnership that should be considered for the GEAR Center will itself be an innovation.

3.1 What sectors, stakeholders, types of expertise, and networks or programs should be involved?

Academia, industry and government agencies, but also public and private (for-profit and non-profit) organizations that are actively capturing and analyzing data, are involved in economic development, research and business incubation efforts should be considered important stakeholders. Those groups describing, developing and deploying technology-based federations. In short, the stakeholders involved should include those that are fueling innovation, those that are shaping how those innovations are commoditized/commercialized, those that are actively engaged in the delivery of services and those entities that fund and allocate resources to all of these efforts.

3.2 What should a governance structure look like or include?

The most appropriate governance structure would be similar to the CBF that was established for the operation of the CSCE. CBF was formed as a non-profit 501c3 and has an Executive Director reporting to the Board of Directors. In addition, there is a Board of Advisors comprised of the major stakeholders in the mission areas of the CSCE/CBF. The GEAR Center should be similarly organized with representation by both the public and private sectors.

3.3 How should the GEAR Center maintain mission focus without the Federal Government being responsible for ongoing administration, staffing, and operational management?

Formal Government sanction for the mission of the GEAR Center along with a contract mechanism to get to the consortium serving the mission of the GEAR Center are critical elements necessary to ensure that the GEAR Center sustains mission focus. Private industry responds best to the knowledge of an actual stated need by the government as well as funding to support the effort.

4.0 What examples already exist that serve a purpose similar to the GEAR Center, whether for governments or other institutions?

The catalyst for the CSCE was to address the paucity of available and qualified cyber security personnel. The CSCE and CBF were borne out of the need to hire these personnel to support contracts being won by XCorp. The discussion expanded to other companies experiencing the same challenge. Discussions with the state and federal government as well as with Department of Defense indicated that the challenge of finding and sustaining qualified cyber security personnel was agnostic to the organization. This primary purpose for the CSCE is what qualifies us to be the pilot GEAR Center.

4.1 How might such examples be replicated, scaled, connected, or more systematically leveraged?

The CSCE can be leveraged today. Effectively, it is operational now with the CBF and plans to move into the new facility in the summer of 2019. The GEAR Center could be fully operational by FY2020, 1 October 2019.

4.2 Opportunities for the Government to learn more about these examples, such as through a demonstration, virtual interaction, or other method.

Relative to the CSCE, XCorp offers to host the Government for a discussion regarding the CSCE and the CBF. We will include the Board of Directors of the CBF and key consortium members for this discussion, particularly those offering core competencies to the CSCE. If interested, please contact Mr. Cesar Nader whose information is provided on the cover sheet to this RFI response.

Establishing the GEAR Center

5.0 What model should be used to establish a GEAR Center, including:

The consortium management model is most appropriate for the GEAR Center. Only members of the consortium would have the opportunity to propose support and/or technologies for a particular stated need by the government. A public sector consortium management entity, such as CBF, would facilitate the responses by the members of the consortium to a Statement of Need issued by the government.

5.1 The most effective and low-burden mechanism to establish a GEAR Center, such as the Government issuing a challenge, pursuing a traditional procurement, or an alternate approach?

The most effective mechanism to establish a GEAR Center is to leverage private industry investment such as that by XCorp in the CSCE. The facility is essentially available now and the new CSCE is under construction. Effectively, a GEAR Center could be operational by Fiscal Year 2019.

Contractually, Other Transaction Authority (OTA) is much more effective than traditional procurement and would serve as a catalyst for member participation in the consortium.

5.2 If the Government were to pursue a challenge or other open competition, the key considerations in establishing a panel of judges?

Understanding the challenges that the workforce faces is critical when considering who should be a judge. It is recommended that not only leadership participate in the panel but also individuals from within each level of the workforce. These personnel would be able to give the clearest perspective on how the reskilling and upskilling approaches would impact their day to day responsibilities and would also allow for understanding what would incentivize the workforce to invest in the process.

6.0 How should a GEAR Center be funded?

The government needs to provide seed funding for 3-5 years which will provide time to establish the private sector management entity, build the consortium, and attract funding from both the public and private sectors. Over time, as the program matures, the Center will likely be funded through other sources such as: fees for services; overhead on innovation related grants (from non-profit and for-profit sources); and, local and state economic development funds supporting commercialization.

6.1 What could be sustainable funding approaches, including sources of funding?

A sustainable approach would be similar to the CSCE, whereby there is a tiered investment strategy in the non-profit management organization. In addition, the management organization would pursue funding from both stakeholder sectors, public and private.

6.2 What market incentives are necessary to make the Center sustainable?

The fundamental market incentive is the correlation of the skills needed by the public sector with those in demand by the private sector. The CSCE supported collaboration among government, academia, and industry related to cyber knowledge, skills, and abilities serves as a proof point for this approach.

Anticipated Early Focus Areas

7.0 What models, approaches, and opportunities should inform an anticipated early focus on reskilling and upskilling Federal employees?

The prioritization of the training of the Federal Workforce must be focused on the professionalization of the Workforce. The skills that are focused on must be ones that demonstrate to the individual that their value is recognized and that the organization is focused on their continued contributions and efforts.

The metrics that are used to assess the effectiveness of the reskilling and upskilling efforts are first the successful completion of the training course assigned with knowledge metrics during the course itself. Upon successful completion of the course the individual then begins their "practice tests" that further measure their knowledge retention and preparedness for the professional certification exam. Only upon successfully passing the practice test with a 90% score or better is the individual provided with a voucher for the actual exam. This methodology resulted in the successful upskilling and professional certification of all but one individual within the reporting environment.

This methodology or process allows for the continued professional development of the workforce by ensuring they have the baseline knowledge required and then bringing the individual through an upskills process focused on currently in demand skills as well as giving the organization the ability to focus select individuals on preparations for future transitions into different technologies.

Recognizing that Machine Learning and Artificial Intelligence (ML/AI) technologies will soon become part of the "workforce" as intelligent automation takes root, it is important to identify as early as possible where emerging ML/AI based technologies will displace the human workforce and target reskilling and upskilling efforts in anticipation of those sorts of displacements.

7.1 What are leading practices for effective reskilling, upskilling, and training adult workers, including opportunities for new applications of existing models?

There should be a balanced approach that recognizes both "continuous learning" along the lines of traditional post-secondary education and targeted skills development that are task, function or technology focused.

Adult workers need to know that their leadership understands that they already have a job to do. Many are fully immersed and dedicated daily to those responsibilities and do not feel that they have the time to also focus on upskilling. This is where our model for online training fits. Instead of taking the individual away from their daily responsibilities for anywhere from 3 days to several weeks, we deliver the training online directly to the student in two-hour blocks of training. Our delivery model for training is a new, highly engaging and interactive online web-based learning series, which eliminates traditional corporate training barriers by enabling students to access the best in live, technical information and certification training anywhere, anytime. This training is scheduled, live courses or pre-recorded courses with the most knowledgeable, real-world experienced instructors. Each class is built with the CGI technology and filled with live video, multimedia presentations, interactive discussion, and includes guest "in the field" experts. This provides a massively engaging, next-generation web training

experience with live instructors. All delivered in a way that is interactive, which helps students learn and apply the concepts to their job immediately without taking them away from their day to day responsibilities. Each course is updated, at a minimum, every six weeks with the latest real-world information ensuring that the students are always on the cutting edge of any transitions in existing or future technologies.

7.2 What approaches could be piloted for possible application and scalability across the Federal sector in various learning domains (e.g., cognitive, affective, behavioral) - such as gamification, use of massively open on-line courses (MOOCs), apprenticeship models, and other new approaches?

Use of gaming-based, individualized and targeted training will be important to "micro reskilling" (highly targeted training and enhanced proficiency development) that can be developed to drive near real-time and continuous learning should be considered.

7.3 What are examples of metrics currently used to assess the effectiveness of reskilling and upskilling efforts?

Game-based performance metrics (skill assessment, proficiency and effectiveness) against defined minimum capability standards would be a useful approach. The purpose of assessment should be to evaluate the readiness of an individual to deliver needed outcomes utilizing a given solution process *and* their ability to adapt to changes in the process or shifting of target outcomes.

7.4 Do any of the suggested approaches have a particular nexus to the Federal workforce and/or to the automation of existing workflows, and transformation of existing skills to in-demand skills expected to comprise the "future of work"?

In addition to training to support emerging workflows, processes and technologies, the Federal (state and local) workforce must be able to also manage the migration from "old legacy" approaches to new current and future ones. The burden on the workforce for the foreseeable future (next decade) is that individuals in transitioning need to be well grounded in both approaches. Otherwise, natural "polarization" in "old" and "new" camps may create friction that slows down change or causes harm through active resistance or unwise aggressive application of new technology without thought to consequence.

8.0 For an anticipated early focus on how Federally owned data could help transform society and grow the economy:

8.1 Are there opportunities for the Federal government to partner with the private sector to improve data architecture/taxonomy, and data quality/hygiene?

Not only are there opportunities to do so, it is now (and likely for the foreseeable future) unavoidable. The sources of data needed for the proper functioning of government and government agencies (the public sector writ large) are increasingly harvested and stewarded by private sector entities. The lack of alignment of data architectures, taxonomies, syntax, quality

and security between and among the governmental, academic and commercial entities will be a major challenge that must be faced and addressed. As an example, consider smart-cities initiatives around transportation (autonomous privately-owned vehicles, public transportation, security, traffic flow management and emergency response capabilities).

8.2 Are there innovative economic models that highlight the value of the data, and would encourage private investment to capture that value both within the Government and across the broader economy? What are the barriers to implementing these models?

A promising approach is to establish data marketplaces that leverage governmental, academic and commercial data providers. It may be useful to allow "free" or low-cost access to data for research and exploratory innovation (since many such data-intensive research projects are federally funded) – but charge a fee for commercial use of such data.

The primary barriers to opening up data access are perceived proprietary value of data, data privacy and data security ("I welcome getting your data, but you can't have mine…"). The interoperability of data harvested from multiple sources is also a real and often poorly understood problem. The Center will need to have some ability to encourage data sharing and data integration through some form of "data fusion" (likely through academic partnerships).

8.3 Are there specific data sets that could be further leveraged by the Federal government, start-ups, and the public – that, once scaled, have a significant potential to contribute to the greater good (bolster the economy, improve population health, provide services to the general public, etc.)?

All data sets would have the potential to contribute. At minimum, the availability of data provides an opportunity to understand where ML/AI technologies are potentially useful and the use of such data to train AIs to support human sorting through data and aligning disparate data sets is essential.