Request for Information (RFI): Establishing Government Effectiveness Advanced Research (GEAR) Center

Supplier Response

PREPARED BY SYNACK, INC.
Date: 09/11/2018
Mark Kuhr, Brett Kozisek
Mike Larmie,
Justine Desmond

Synack

Synack, co-founded by two former NSA operators in 2013, is the market leader in crowdsourced penetration testing. Through our collective past experience working with the DoD on projects like Hack the Pentagon, the Intelligence Community (IC), federal civilian agencies, and large commercial enterprises like Domino's and Santander, Synack assessments have helped customers protect their high-value assets with more efficiency, control, and ROI than standard testing or bug bounty alternatives.

Mark Kuhr
Dr. Kuhr co-founded Synack after focusing over nine years on Cyber Security in Academia and Defense industries. Most recently, at the National Security Agency (NSA), Dr. Kuhr worked in roles that include Technical Director, Computer Network Operations Operator, Network Analyst, and Computer Scientist. Dr. Kuhr received a Ph.D. in Computer Science from Auburn University under a DoD/NSA-sponsored fellowship.

Email: mark@synack.com

Brett Kozisek
Mr. Kozisek is the Director of Federal Sales for Synack. Mr. Kozisek has over 25 years as an experienced Sales Leader and Sales Professional who has successfully worked with a wide range of emerging Information Technology companies that have become dominant players in the Public Sector and Commercial enterprise market. He actively took part in the expansive growth in the Federal space with companies like BlueCoat, NetWitness, FireEye, and Invincea.

Email: bkozisek@synack.com

Michael Larmie
Mr. Larmie is the Federal Solutions Architect for Synack and works with all United States Federal, Civilian, DoD, and Intel Agencies providing crowdsourced security penetration testing solutions for all agencies. Mr. Larmie has worked as a Federal Agency Security Subject Matter Expert (SME) for several private industry companies such as G2, Inc, Rapid7, Infoblox, Sourcefire, Tenable Network Security, and Fidelity Investments with a total of 22 years of cybersecurity experience.

Email: mlarmie@synackinc.com

Justine Desmond
Ms. Desmond leads federal, state and local government marketing at Synack. Prior to working at Synack, she was on the original team at PUBLIC, a London-based firm that provides funding, networks, and insight to help technology firms work more deeply with the UK's public services. She also worked at the US House Committee on Foreign Affairs and US House Committee on Science, Space, and Technology. She has an MPA from the London School of Economics in Economic Policy.

Email: jdesmond@synack.com

Synack's Public-Private Workforce Partnerships

Synack helps organizations with the full spectrum of their security testing needs. We harness the world's most exclusive team of security researchers and give them access to a powerful platform for trusted security testing. That testing yields vulnerabilities, data to measure attack surfaces, and provides documentation to aid compliance. Synack testing is designed to make organizations' more resistant to attackers, before they can exploit vulnerabilities to breach customer data, steal money, or worse.

More recently, Synack has sharpened its platform's capabilities for training and educational purposes through a number of public-private partnerships. We aim to bring some of Silicon Valley's focus on efficiency, talent, and innovative technology to Washington, DC. We are aggressively piloting new training models to help support the federal government in its efforts to scale its cybersecurity workforce through the following avenues:

- Together with a federal government agency, Synack is implementing our platform as a training tool for "blue teams" as way to process and vet skills. Blue teams are made up of security engineers who perform analysis of information systems to ensure that they are secure.
- Synack has also experimented with embedding client testers alongside Synack's Red Team, our skilled ethical hackers, through its engagement with Department of Defense as a way to help train soldiers on offensive cyber techniques.
- We are in the process of developing a standalone training product for training institutions (both within government and outside government).
- Synack has led on pro bono initiatives alongside Army Cyber, and R00tz, a nonprofit that teaches kids hacking techniques, and its Synack Red Team on a local level to help educate youths and top students about informal, hacking skills needed to succeed in the cybersecurity field.

At Synack, we are committed to protecting the American Way and maintaining a competitive edge in our 21st Century workforce. We look forward to finding ways to work with the OMB to support the GEAR Center. We agree with Suzette Kent that the federal government needs to support "the [development of] skills the employees need to have to be successful in the environment they're working in" (Nextgov, 2018).

Synack has provided some initial thoughts and ideas for question's #1 and #3 and #7. Several attachments are included as well.

Synack's Responses to the RFI: Establishing a Government Effectiveness Advanced Research (GEAR) Center

Questions

1. Given the mission of the GEAR Center, what should be:

- Its strategic approach and operating objectives?
    - Despite high demand for efficient and effective cybersecurity training solutions due to in large part to a security talent shortage in the federal government, we've seen little innovation in workforce training.
    - Synack recommends including cybersecurity training as one of the Gear Center's objectives. The Gear Center could host cybersecurity education seminars, practical skill assessments, and hands on workshops. These would focus on both Offensive and Defensive network security training. This type of hands on training could include "Blue team" and "Red Team" training and real time scenario-based drills that would allocate the Blue team and Red team to different cyber challenges.
    - Synack would recommend a track on how to assemble penetration testing that utilizes internal resources and crowdsourced partners that a Federal Agency could promote, implement, establish, and conduct. These challenges could include both external and internal assessments.

- Specific areas of innovation and practice to prioritize? For example, we anticipate an early focus on reskilling the Federal workforce and growing the economy through appropriate commercialization of Federal data.
    - Synack advises that an area of innovation to prioritize is opportunities for learning "informal" skills in computer network cybersecurity offensive hacking to increase the knowledge.
    - Building a training center that can accommodate and host an environment to run simulated environments will allow government workers to get hands on practical experience necessary to develop best in class cyber security skills.
    - Synack's scalable software platform provides maximum accessibility to a large workforce, with the added benefit of realistic testing of selected government assets.
        - Hands-on, practical experience is critical to developing the offensive and defensive cyber capabilities required of today's cyber corps. Historically, these realistic training opportunities have been limited in pragmatism and availability.
        - This approach will ensure that the top cyber talent is quickly identified and developed through hands-on experience, performance measurement and benchmarking, and regular mentorship.
        - This talent development is made possible through this crowdsourced security testing platform that enables testers with technology, tracks and

        monitors testing activity, and provides real-time feedback through analytics and reporting.
        - Based on prior experience training and testing organizations, one year should provide ample time to identify, develop and motivate the top 10% of cyber specialists in the government, with the additional benefit of penetration testing of chosen targets on-demand and at scale.

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

    - Synack understands that innovation and workforce training are broad themes that are cross-cutting across the United States government, but cybersecurity training specifically should be a focus.
    - One of the key challenges is little knowledge of government workers' aptitudes for precise cybersecurity skills and training since the field is very broad. A testing center could assess the current capabilities of personnel and help shape the focus in future.
    - Synack suggests a cyber security skills assessment focus area where personnel could showcase their current skill set and then apply for specific training in different areas of cyber security. Examples could be web-based penetration testing, mobile device assessments, operating system assessments, Internet of Things (IoT) assessments, and more.
    - Synack recommends diverse education tracks in cyber security including: offensive network training, defensive network training, digital forensics training, mobile device security training, and IoT training with different areas of focus from beginner to advanced, to include live exercises and on hands development in each focus area and skill level. The education tracks should also encourage professionals to take one or more or mix their skill sets to have a very diverse learning experience.

3. What models of public-private partnership should inform the GEAR Center:

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

    - Synack recommends a focus on cyber security for both offensive and defensive focus areas.
    - Synack recommends a program on penetration testing and secure crowdsourced penetration testing for the US Government.
    - Synack recommends creating a center for monitoring vulnerability submissions and triage support for handling incidents that are submitted publicly to a US Government Agency.

7. What models, approaches, and opportunities should inform an anticipated early focus on reskilling and upskilling Federal employees? For each question, please cite any available data or research to support your answer.

- What are leading practices for effective reskilling, upskilling, and training adult workers, including opportunities for new applications of existing models?
    - Synack would recommend cyber security tracks and updating the material from existing network engineering and physical security training.
    - Adopt and assess skill level of workers that would apply based on any computer experience level and provide them with a roadmap to get their skill sets aligned with subject matter areas such as network scanning, vulnerability scanning, identification of security threats and industry leading tools - and opt to using open source tools for providing hands on educational capabilities for training adult workers.
- 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?
    - Synack would recommend a specific training area in crowdsourcing at scale to solve challenges beyond small teams. This training area may include an in-person, or on-line mentorship program.
    - Top cyber security experts from Synack could act as mentors and will act as assessment leads working with groups of candidates to advance their skillsets. Mentors will work with candidates to set performance objectives, track performance over time, and provide regular trainings on specific techniques, tools, and tactics in order to help candidates achieve their goals.
- What are examples of metrics currently used to assess the effectiveness of reskilling and upskilling efforts?
    - Crowdsourced security also has universally agreed upon metrics that can help judge the progress of prospective government employees
        - Attacker Cost - the level of effort to find vulnerabilities
        - Severity of Findings - severity and quantity of vulnerabilities found
        - SRT Skill - an assessment of the complexity of the vulnerability based on the tester skill required to find it.
        - While candidates are working on testing target systems, a crowdsourced cadre of expert security researchers will be working alongside them. This cadre will provide a sufficient skills benchmark for the candidates and allow management to measure effectiveness against a set of expertly skilled researchers in a specific technology area. Since all users will use the platform, which records full testing activity, the same parameters of tools, time, tradecraft and techniques can be used as comparison points.

- 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"? If there are occupations or skill sets that would provide an opportunity-rich environment, please include specifics.
    - There are many potential models, approaches, and opportunities, but the ones we can speak to apply to the cybersecurity realm.
    - Only by training on simulated real-world targets and diverse environments will the candidates' get hands on practical experience necessary to develop best in class cyber skills
    - Should our federal government pilot for training and skill vetting be a success, crowdsourced security training could be piloted across federal government. Each department and often agencies have a CIO or CISO that has a direct need to train veterans and also train new employee talent. We are ready to help to fill that need.