RapidFort, Inc
2 Townsend St 1-303
San Francisco, CA 94107
5 April, 2021
Russ@rapidfort.com
Ph (415) 837-3076

Hing Pan Wong
National Institute of Standards and Technology (NIST)
Acquisition Management Division,
100 Bureau Drive, Mail Stop 1640,
Gaithersburg, MD, 20899-1640

Dear Sir/Madam:

SOURCES SOUGHT NOTICE: CYBER SUPPLY CHAIN RISK REDUCTION

Document Type: Sources Sought Notice
Notice Number: AMDTC-21-0002
Title: NIST Cybersecurity and Privacy Support Services (CAPSS)
NAICS Code: 541519 – Other Computer Related Services

We would like to respond to the following topic area:

3 PRIORITY: HIGH ---- Research work to be conducted in the following areas. Specifics in each TO.
b. Cyber supply chain risk management

We have a developed a platform that revolutionizes the ability to reduce software supply chain risk by automatically removing container vulnerabilities at the click of a button. There are a variety of other unique features.

We would welcome the opportunity to discuss and/or present our results to any party at NIST interested in reducing software supply chain risk.

Our Name, Address, DUNS number, CAGE code, and point of contact information of our company is on the last page of this document.

Please can you forward this note onto NIST parties interested in Reducing Software Supply Chain Risk.

Sincerely,

Russell Andersson

Russell Andersson
Chief Commercial Officer, CAIA

CC: Keith Bubar, keith.bubar@nist.gov, tel:3019758329

EXECUTIVE SUMMARY:

- RapidFort (RF) is a team of engineers based in Silicon Valley, who have developed next generation software supply chain risk reduction technologies.
- Modern computing is moving to cloud based technologies that have numerous advantages.
- But these cloud-based technologies also have innate weaknesses that enable exploits like SolarWinds and Microsoft Exchange Server breaches. These breaches are called Software Supply Chain Exploits and Zero Day Exploits specifically. (These events have been labelled as Software Supply Chain Risk for SolarWinds because the exploit was introduced upstream in the software supply chain. And Zero day for Microsoft because the vulnerability was known for zero days before it was exploited).
- These breaches have had significant consequences for national security and have heightened congressional and presidential tension with nation states like Russia and China.
- Regulatory agencies have made sweeping regulatory changes to reduce software supply chain risk with FEDRAMP announcing new container scanning regulations on 16 March 2021. CMMC requirements already include scanning but the intensity of the scanning requirements maybe increased imminently.
- Further increased supply chain cybersecurity requirements, to address these risks, are expected in a **Presidential Executive Order** expected within the next 28 days.
- There is a huge amount at stake and the situation is serious.
- Fortunately, RF has created a patent pending, unique, extremely effective, solution to address software supply chain risk(s) and zero-day exploit risk(s).
- RF scans a container and can automatically remove vulnerabilities and unused code.
- This technology is a game changer and can dramatically reduce software supply chain risk by automatically removing software vulnerabilities at the touch of a button within a few minutes.
- In a small Proof of Concept for the USAF, the vulnerabilities were reduced by **82%** and the attack surface by **78%**.
- The Chief Software Officer of the USAF described the technology as **"very impressive."** As a result, RF received Funding on 26 March 2021 to deliver a specialized customized solution to the USAF software factory community who use a specialized DoD cloud called PlatformOne.
- RF is seeking to demonstrate the technology to NIST to explore how it can be employed more broadly to reduce cyber software supply chain risk for the US technology community at large.
- RF has a variety of potential uses cases it would like to present to NIST specialized focused on software supply chain risk.

CLOUD BASED TECHONOLOGIES, CONTAINERIZATION, AND SOFTWARE SUPPLY CHAIN RISK:

- Most modern cloud-based infrastructure runs on software containers because they tend to be easier, faster, and cheaper to build and less expensive to run.
- Containerization places all the necessary software into a "container" so that the container has everything it needs to run on practically any infrastructure. The "container" "contains" everything it needs in a complete package, hence the name.
- Because all the software components are bulk loaded, when it is containerized, one of the biggest issues of containerization is that 85% to 90% of the software in the container is not used. Containerization only tends to work well in one direction: easy to put in, very hard to take out.

- While Containers have multiple benefits, in terms of speed, cost, and performance containers this "load-everything" approach has 2 significant cybersecurity drawbacks because:
    - **Firstly,** this is much more software inserted and this creates Software Supply Chain Risk whereby malicious components can be inserted and exploited to enable breaches. Its so much easier to slip in a package if the total number of packages in the container/application is much larger. (The SolarWinds Breach was an example of Software Supply Chain Exploit a package was slipped into the supply chain upstream that allowed firewalls to be compromised).
    - **Secondly,** the increased size of the code base enables Zero Day Exploits, where undocumented and unknown vulnerabilities, that only hackers are aware of, can be exploited to create breaches. Because there is simply much more software to attack there is more software surface to attack. (The Microsoft Exchange Server Fiasco was a recent example of A Zero Day Vulnerability Exploit. There was an undocumented vulnerability that was leveraged to enable significant damage)
- Of increasing concern, is that now the supply chain attack vector has been proven to be viable by opposing nation states, it is possible that even more attacks are coming from criminal actors who will copy the techniques the nation state actors have pioneered.
- To defend against these weaknesses, the current state of the art is to SCAN software to identify vulnerabilities. Once the vulnerabilities are identified through scanning they are then manually fixed and/or removed. This removal process can take months.
- But scanning only IDENTIFIES risks it doesn't RESOLVE them.
- SCANNING alone also does not solve the zero-day exploit code issue because the rest of the software remains in place and is vulnerable to attack.

THE RAPIDFORT SOULTION IS A GAME-CHANGER:

- RapidFort has developed industry leading next generation technology that not only SCANS, but PROFILES AND then REMOVES the unused code automatically. This process can be done in minutes as part of a traditional software build cycle, most notably through CI/CD tools.
- This approach is patent pending, revolutionary and unique. Rather than identify, then fix the vulnerabilities, the software container is profiled to understand all the code that is required, and if it is not required, it is removed. Hackers can't hack code that isn't there.
- This approach not only removes the vulnerabilities that were detected but it also removes risks in the software that didn't scan positive.
- With all other solutions the ability to remove vulnerabilities is a function of the quality of the scanning and the quality of the databases used to cross reference packages against vulnerabilities.
- But with the RF approach the software is removed regardless of the quality of the scan.
- This is why the technique is so powerful.
- In terms of reduction of zero-day exploits, it's a total game changer. There is no other solution we are aware of that addresses zero-day risks as comprehensively.

ALREADY SUCCESSFULLY ENGAGED WITH THE USAF:

- In January 2021, RapidFort conducted a Proof-of-Concept test against USAF containers and reduced vulnerability counts by **82%** and reduced vulnerabilities by **78%.** Less code, means less risk.

- These results were demonstrated to the Chief Software Engineer of the USAF. After writing a strong Memorandum of Support, a technical evaluation and competitive analysis was done by USAF technologists, who then wrote a favorable recommendation.
- As a result of this support from within the USAF community, on 26 March 2021, RapidFort was granted an SBIR Phase 1 to deploy its technology on PlatformOne where it can be used by USAF Software Factories developing code.
- To meet the high USAF configuration standards, RF needed to re-architect minor elements of its product, with the expectation that RapidFort will be live on PlatformOne in late May 2021.
- RF expects CMMC Level 1 Certification will be forthcoming shortly thereafter.

SEEING IS BELIEVING:

- RapidFort has developed a game-changing solution to reduce Software Supply Chain Risks, and reduce the potential for Zero Day Cyber Attacks.
- These are bold claims. Current users describe RapidFort as being "like magic" and "1000 light years ahead."
- We respectfully request the opportunity to demonstrate the technology to any party at NIST interested in seeing it. To the extent it is benefitial, NIST technologists can provide their own containers. RapidFort will harden them, and within a few minutes one can see for oneself if the vulnerabilities have been removed, and the container performs to specification.
- The expectation is that the vulnerability reduction will be in the **60% to 90%** range largely dependent on language and components being used. With JavaScript applications the vulnerability removal rates can be above **95%.**
- There is nothing else commercially available that is remotely as effective. The technology is game-changing and works as advertised.

POTENTIAL AREAS OF COLLABORATION:

- The platform has a number of other software supply chain benefits
- There are a number of areas for potential collaboration.
- RF would be willing to make the scanning solution available to NIST for free, for example.
- We also have projects in place to:
    - Risk score vulnerabilities using a ML algorithm.
    - To risk score the total supply chain risk in a container.
    - To risk score the total supply chain risk in an application.
    - To predict when proof of concept exploits will take place.
    - To predict when fixes will become available.
    - To predict how many vulnerabilities can be automatically removed.

RESPONDING TO SOFTWARE SUPPLY CHAIN RISK IS VITALLY IMPORTANT:

- We would love to engage with NIST to provide more clarity into state-of-the art software supply chain technologies.
- We stand ready to demo the scanning solution. Benchmark it against comparative systems. Conclusively prove it works. And demonstrate its value.
- And we'd love to profile some up and coming projects relating to risk scoring supply chain risk.

- If the technology works as advertised the benefits will be significant.
- We want to contribute and we'd welcome the opportunity to present a more detailed proposal and validate our claims.
- We'd hope we have made a sufficiently strong case that further evaluation of the proposal is justified given what is at stake.

COMPANY BACKGROUND INFORMATION:

- **RapidFort Address:** 138 Kensington Way, San Francisco, CA 94127
- **DUNS Number:** 11 785 3370
- **CAGE Code is: 8U9L6**
- **Small Business Administration Small Business Concern ID # is:** SBC_001870615
- **Any information on the company's small business certifications, if applicable.**

  We expect to be certified in a CMMC level 1 equivalent to offer our services on PlatformOne.

- **Description of your company's capabilities as they relate to the services described in this notice**

  RapidFort has developed a comprehensive platform to dramatically reduce Software Supply Chain Risk.

- **A description of your company's previous experience providing the services described in this notice.**

  We are in the process of taking a similar project live for the USAF, with a number of other engagements with large high profile civilian organizations.

- **5. Indication of whether the services described in this notice are currently offered via your company's GSA Federal Supply Schedule (FSS) contracts, Government-wide Acquisition Contracts (GWACs), or other existing Government-wide contract vehicles; and, if so, the contract number(s) for those vehicles.**

  We do not have a GSA contract but would be willing to provide the platform to NIST for free so perhaps a contract is not required.

- **6. Any other relevant information that is not listed above which the Government should consider in finalizing its market research.**

  We have done a comprehensive study of solutions in this space and would be happy to share our findings with the NIST team.