STATE OF TENNESSEE
DEPARTMENT OF FINANCE & ADMINISTRATION

REQUEST FOR INFORMATION
FOR
DDoS Mitigation Tools

RFI # 31701-03595
1/24/2025

1. STATEMENT OF PURPOSE:

The State of Tennessee, Department of Finance & Administration – Strategic Technology Solutions issues this Request for Information ("RFI") for the purpose of researching DDoS mitigation tools. We appreciate your input and participation in this process.

2. BACKGROUND:

The State of Tennessee recognizes the increasing sophistication and frequency of Distributed Denial of Service (DDoS) attacks, which pose a significant threat to the availability and integrity of critical government services. To proactively mitigate these risks and ensure the continued delivery of essential services to citizens, the State is seeking information from qualified vendors regarding their DDoS prevention capabilities and solutions.

3. COMMUNICATIONS:

3.1. Please submit your response to this RFI to:

Chris Romaine, MBA | Contract Specialist
901 Rep. John Lewis Way North, Nashville, TN 37243
Cell: 615-913-2407
Christopher.Romaine@tn.gov

3.2. Please feel free to contact the Department of Finance & Administration – Strategic Technology Solutions with any questions regarding this RFI. Questions should be directly emailed to the main point of contact by the deadline listed below in Section 5. RFI Schedule of Events.

3.3. Please reference RFI # 31701-03595 with all communications to this RFI.

4. RFI SCHEDULE OF EVENTS:

EVENT		TIME (Central Time Zone)	DATE (all dates are State business days)
1.	RFI Issued		1/24/25
2.	Written Questions & Comments Deadline	2:00 PM	1/31/25
3.	State Response to Written Questions & Comments		2/5/25
4.	RFI Response Deadline	2:00 PM	2/14/25
5.	Complete Review of Responses		2/24/25
6.	Schedule Demo Sessions		2/26/25
7.	Conduct Virtual Demos / Q&A Sessions		3/4/25 - 3/6/25

5. GENERAL INFORMATION:

5.1. Please note that responding to this RFI is not a prerequisite for responding to any future solicitations related to this project and a response to this RFI will not create any contract rights. Responses to this RFI will become property of the State.

5.2. The information gathered during this RFI is part of an ongoing procurement. In order to prevent an unfair advantage among potential respondents, the RFI responses will not be available until after the completion of evaluation of any responses, proposals, or bids resulting from a Request for Qualifications, Request for Proposals, Invitation to Bid or other procurement method. In the event that the state chooses not to go further in the procurement process and responses are never evaluated, the responses to the procurement including the responses to the RFI, will be considered confidential by the State.

5.3. The State will not pay for any costs associated with responding to this RFI.

5.4. Any services or products proposed in this RFI, must be in compliance with the following security policy: all State data must remain in the United States, regardless of whether the

data is processed, stored, in-transit, or at rest. Access to State data shall be limited to US-based (onshore) resources only. Configuration or development of software and code is permitted outside of the United States, however, software applications designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary, which the U.S. Secretary of Commerce acting pursuant to 15 C.F.R. 7 has defined to include the People's Republic of China, among others are prohibited. Any testing of code outside of the United States must use fake data. A copy of production data may not be transmitted or used outside the United States.

5.5. The State may request demo presentations from select RFI respondents.

5.6. Responses should be prepared, with emphasis on completeness and clarity, and should NOT exceed twenty (20) pages in length. Attachment 1 is not counted towards the page count. Responses, as well as any reference material presented, must be written in English, and must be written on standard 8 ½" x 11" pages and all text must be at least a 12-point font. All pages must be numbered.

6. INFORMATIONAL FORMS:

The State is requesting the following information from all interested parties. Please fill out the following forms:

RFI # 31701-03595 INFORMATIONAL FORM - Functional Requirements
1. RESPONDENT LEGAL ENTITY NAME:
2. RESPONDENT CONTACT PERSON: Name, Title: Address: Phone Number: Email:
3. Brief description of experience providing similar scope of services/products
4. Describe how your solution detects and mitigates Layer 6/Layer 7 application layer attacks.
5. Describe how your solution enables detection and mitigation of Layer 4/Layer 5 protocol attacks that cause resource exhaustion.
6. Describe how your solution detects and mitigates Layer 3 volumetric attacks. (ICMP floods, SYN foods, DNS amplification attacks, UDP floods, and IP fragmentation attacks)
7. Describe how your solution provides easily understood, friendly interfaces with intuitive designs to facilitate user engagement.
8. Describe how your solution supports highly distributed edge-based cloud delivery platforms that provide content acceleration, API caching, image optimization, streaming video delivery, web application and perimeter security, and edge compute and storage. (Protect any State infrastructure regardless of location.)
9. Describe how your solution enables a real-time logging and reporting interface.
10. Describe how your solution supports a security operations center and managed security services.
11. Describe how your solution blocks in-bound patterns form automated bad bot attacks.
12. Describe how your solution protects Domain Name System (DNS) infrastructure from cyber intrusions.
13. Describe how your solution enables protection of web applications and application programming interfaces (APIs) from cyber-attacks and other intrusions.
14. Describe how your solution traffic filtering to block known Bad IP addresses (Bad Monkey List)
15. Describe how your solution access to real time network traffic dashboards.
16. Does your solution offer actual human contacting customer care center via phone call. (SMS, Email, Logging).

RFI # 31701-03595 INFORMATIONAL FORM - Technical Requirements
17. Is it possible for your solution to maintain provider logs for 6 months and give the State access to logs.
18. Can your solution integrate with all relevant applications, data sources and technologies and migrate logs to Splunk SIEM.
19. Describe how your solution provides proactive alerts on system events and enables logging and resolution reporting on all issues.
20. Describe how your solution enables configurable controls that extend data and transaction security and compliance to third-party platforms or the solution's hosting providers. How do you document security policies, audits, attestations or evaluations for compliance needs.
21. Describe how your solution enables processes such as disaster recovery, rollbacks, and version control for configuration and console items. (High Availability)
22. Describe how your solution supports capabilities such as user authentication, password policy management, two-factor authorization, single sign on and role-based access in a Break Glass account or Super admin Account.
23. Describe how your solution leverages network technologies like software-defined wide area networks and over-the-top monitoring to ensure the optimal performance.
24. Describe how your solution complies with relevant standards like CCPA, GDPR and third-party or government certifications such as SOC 2/Type 2, ISO 27001 and FedRAMP.
25. Describe how your solution allows customization of the standard deployed solution with custom user interfaces, data tables, process components and business logic.
26. Describe how your solution supports off-the-shelf localization such as insights, language, and currency support for required geographies.

RFI # 31701-03595 INFORMATIONAL FORM - Support and Services
27. Describe how you deliver the required level of user and technical support, e.g., 24/7, 365 nights and weekends. multi-language and global support.
28. Describe how you provide implementation resources (including setup, testing, and training) to meet a desired go-live date.
29. Describe how you will provide a clear implementation plan and resourcing (including setup, testing and training) to meet a desired go-live date.
30. Describe how you provide support across multiple formats including phone, email, chat, and online knowledge base. Will you contact the State using the same available formats?
31. Are you able to provide clear rollout options such as staggered, proof of concepts or end-to-end enterprise deployments.
32. Are you able to meet relevant service level agreements related to system performance, concurrent users, uptime, and issue resolution. Are you able to meet SLAs associated with support request.
33. Describe how you provide best-in-class training and assistance for users using online and offline mediums.

34. Describe how you may use expertise via vendor or partners to deliver implementation objectives.

INFORMATIONAL FORM – Pricing and Terms
1. Describe what pricing units you typically utilize for similar services or goods (e.g., per hour, each, etc.:
2. Describe the typical price range for similar services or goods.
3. Describe initial contract term including, where applicable, implementation periods and billing start dates. Defines how renewals occur if automatic, notice periods and how terms, pricing or other contracted components such as functionality can change.
4. Describe any licensing pricing units (e.g. number of users, sessions or API calls), cost of each, and forecast annual and/or monthly volumes.
5. Describe Cost to implement and deliver software into full production using either vendor or partner resources.
6. Describe expenses to train and support current users for launch, provide their continuing education and onboard future new users.
7. Provide key terms such as price protection, termination clause, and limitation of liability.
8. Describe fees related to ongoing support services and maintenance, including tiers and precise deliverables.
9. Describe any alternate payment methodology for the solution.

INFORMATIONAL FORM – Additional Considerations
1. Please provide input on alternative approaches or additional things to consider that might benefit the State: