U.S. General Services Administration

Application Security Testing (AST): Acquisition and Adoption

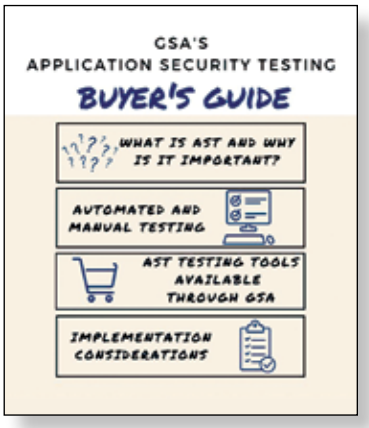
Why is AST Important?

According to the 2022 Verizon Data Breach Investigations Report[1], application hacking is the number-one attack vector, with most security incidents occurring at the application layer. Federal agencies must look past traditional network security technologies to address the modern-day threat of vulnerable applications. Application Security Testing (AST) is one part of an agency's layered approach to securely develop and maintain applications in support of the Administration's strategy of "Improving the Nation's Cybersecurity": **www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity**.

Agencies must follow reporting and testing requirements such as:

- Office of Management and Budget (OMB) Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles": **www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf**
- National Institute of Standards and Technology (NIST) Special Publication 800-218, Secure Software Development Framework (SSDF) Version 1.1: "Recommendations for Mitigating the Risk of Software Vulnerabilities": **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf**.
- NIST Internal Report 8397, "Guidelines on Minimum Standards for Developer Verification of Software": **https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8397.pdf**
- Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 20-01 "Develop and Publish a Vulnerability Disclosure Policy" (**www.cisa.gov/binding-operational-directive-20-01**) and BOD 22-01 "Reducing the Significant Risk of Known Exploited Vulnerabilities" (**www.cisa.gov/binding-operational-directive-22-01**)

Each agency may have a different approach to choosing which of the multitude of services align best with their AST program. **GSA's "Application Security Testing (AST) Buyer's Guide"** provides information on best practices, services to consider, and tools to help your procurement process. To read the guide, visit **www.gsa.gov/ast**.



[1]2022 Verizon Data Breach Investigations Report. May 25, 2022, **www.verizon.com/business/resources/T8ea/reports/dbir/2022-data-breach-investigations-report-dbir.pdf**

AST Key Considerations

- An AST program focuses on aligning people, processes, and technology to continuously assess and address the threat, vulnerability, and overall risk exposure of an organization's internal and external applications, as well as its underlying platforms.
- It is more efficient to invest in early and continuous AST than to risk the potential loss of sensitive data or cessation of operations.
- Most organizations use a combination of manual and automated AST methodologies to test, analyze, and report on the security level of an application.
    - **Manual testing** is executed by human security testers to discover complex bugs for which automated testing cannot scan or to resolve automated testing's false positives. It requires a substantial level of expertise, effort, and time.
    - **Automated AST** relies on written code/test scripts and tools to test and validate an application. It can be completed in less time than manual testing and covers more test permutations; however, it does require heavy coding and maintenance.

Easy Ordering

Your agency can buy AST products and services through the Multiple Award Schedule (MAS) Information Technology (IT) category.

You can also buy AST services through:

- Alliant 2
- 8(a) STARS III
- VETS 2
- Highly Adaptive Cybersecurity Services (HACS)
- Enterprise Infrastructure Solutions (EIS)
- Wireless Mobility Solutions (WMS)

Agencies can leverage GSA's MAS to establish Blanket Purchase Agreements (BPAs). BPAs give agencies a simplified method to fill anticipated repetitive needs for AST services.

Acquisition flexibilities are available to agencies, such as those outlined in FAR Parts 16.603 (**www.acquisition.gov/far/16.603**) and 18 (**www.acquisition.gov/far/part-18**), to facilitate and expedite the acquisition of products and services needed to defend against or recover from cyberattacks.

Government organizations can purchase products, services, and solutions through GSA's technology purchasing programs, including eBuy (**www.ebuy.gsa.gov**) and GSA Advantage!® (**www.gsaadvantage.gov/advantage/ws/search/itsecurity**). You can also issue a Request for Information (RFI) or Request for Quotation (RFQ) and allow vendors to respond to your requirements.

- To find out more, visit **www.gsa.gov/technology/technology-programs**.
- State and local governments can buy GSA technology solutions through the MAS IT category by using the GSA Cooperative Purchasing Program.
- To find out whether your government entity qualifies, refer to the Cooperative Purchasing FAQ: **www.gsa.gov/stateandlocal**. For more information about ordering for state and local governments, visit **www.gsa.gov/portal/content/141511**.

For More Information

The GSA IT Category team is available to answer questions and provide subject-matter expertise related to any aspect of AST and other IT needs.

To learn more about GSA's cybersecurity programs, please visit **www.gsa.gov/cybersecurity**.

If you have any other questions about GSA or AST, please contact the IT Customer Service Center at 855-ITaid4U/855-482-4348 or itcsc@gsa.gov.

www.gsa.gov
January 2023
05-23-00336

View, download, and order publications via www.gsa.gov/cmls.