VENDOR STIG INTENT FORM

***** PLEASE READ *****

PURPOSE: This form is used to notify DISA of a vendor's desire to create a STIG through the Vendor STIG process.

INSTRUCTIONS: Complete this form in its entirety and return to DISA. Send the completed form and any additional correspondence concerning the form or the Vendor STIG process electronically by clicking the submit button at the bottom of this form. Forms will be sent directly to **disa.stig_spt@mail.mil**. Please save or print a copy for your records. Following internal review, DISA will notify the vendor of whether the vendor will proceed to the STIG development process.

DISCLOSURE: Disclosure of this information is voluntary; however, ALL fields MUST be completed before submission to be considered for STIG development. Failure to provide any of the requested information will prevent further processing of this request and will not be considered for STIG development.

PART I *(Vendor Contact Information)*

1. VENDOR NAME *(Requestor)*	2. DATE	3. VENDOR POINT OF CONTACT *(POC)*

4. POC PHONE	5. POC EMAIL ADDRESS

PART II *(Product Information)*

6. PRODUCT NAME *(Subject of proposed STIG)*	7. PRODUCT VENDOR

8. PRODUCT VERSION	9. PREVIOUSLY WORKED WITH APL Yes ☐ No ■

10. PRODUCT AND ADMIN/SECURITY GUIDE URL *(configuration guidance can be sent as an email attachment)*

11. BRIEF PRODUCT DESCRIPTION

PART III *(Components of the Product)*

12. OPERATING SYSTEM	13. DO YOU HAVE AN SBOM YOU CAN PROVIDE Yes ☐ No ■

14. VIRTUAL SOFTWARE	15. WEB SERVER

16. CLOUD SERVICE	17. DATABASE

PART IV *(Sponsor Information)*

18. DOD SPONSOR	19. SUBORGANIZATION

20. SPONSOR POC NAME	21. SPONSOR POC PHONE	22. SPONSOR POC EMAIL

PART V *(Additional Information)*

23. HOW IS THE SYSTEM USED? (*Explain: SaaS, PaaS, client/server, browser access, individual use, device, etc.)*	24. LIST ALL OTHER DOD ORGANIZATIONS WHERE PRODUCT IS CURRENTLY BEING USED *(Optional to include POCs)*

25. TOTAL NUMBER OF LICENSES, COPIES, DEVICES USED IN THE DOD _____

AMOUNT TYPE *(Select One)* Actual ☐ Estimate ■

Submit

VENDOR STIG INTENT FORM

***** PRODUCT APPROVAL DISCLAIMER *****

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which support system Assessment and Authorization (A&A) under the DOD Risk Management Framework (RMF). DOD Authorizing Officials (AOs) may contact disa.stig_spt@mail.mil and request available vendor confidential documentation for a product that has a STIG. This documentation is not published for general access to protect vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with DoD policy and through RMF risk acceptance. Input into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards