**Vendor STIG Intent Form**

**Purpose:**

This form is used to notify DISA of a vendor’s desire to create a STIG through the Vendor STIG process. Upon receipt of the form, DISA will provide the vendor a ticket number to track the effort. Following internal review and acceptance, DISA will contact the vendor to initiate the development process.

**Instructions:**

Complete this form and return to DISA. Send completed forms and any correspondence concerning the form or the Vendor STIG process to the following email address:

<mailto:disa.stig_spt@mail.mil>

|  |  |
| --- | --- |
| **Vendor**  The name of the Vendor proposing STIG development. |  |
|  | |
| **Point of Contact**  The individual DISA will contact to discuss the proposed STIG development. |  |
| **Name** |  |
| **Phone Number** |  |
| **E-mail Address** |  |
|  | |
| **Product**  The subject of the proposed STIG. |  |
| **Vendor**  The product vendor may be different from the vendor proposing to develop the STIG. |  |
| **Name** |  |
| **Version** |  |
|  | |
| **Relevant SRG(s)**  List the Security Requirements Guides to be used as a basis for STIG development. The list of published SRGs is available at <http://iase.disa.mil>. The list of requirement sources will be discussed and adjusted at the beginning of the development process. |  |
|  | |
| **Date considerations** (optional)  If the vendor has any special time constraints they should be listed here. This information may be used for prioritization of efforts. |  |
|  | |
| **DoD Sponsor**  This information may be used for prioritization of efforts. |  |
| **Name** |  |
| **Organization** |  |
| **Phone Number** |  |
| **E-mail Address** |  |
|  |  |
| **DoD Organizations where product is currently installed.** |  |

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 request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig\_spt@mail.mil. This documentation is not published for general access to protect vendor's proprietary information.

AOs have the purview to determine product use/approval IAW 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
* DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04