

TALKING PAPER
ON THE
REQUIREMENTS FOR VENDOR SECURITY BASELINE ASSESSMENT

PURPOSE:

Provide background information for vendors to complete the preliminary documents required to support the Defense Information Technology Certification & Accreditation Process (DITSCAP) and the Air Force Certificate of Networthiness (AF CoN) process. DITSCAP is required to place any "system" on the Air Force Enterprise Network; completion of these requirements is not a guarantee that the vendor will ultimately receive the required milestone of an AF CoN, however failure to provide the documents will slow down or make DITSCAP and an AF CoN difficult, if not impossible.

DISCUSSION

- Vendor Security Document Example Outline
 - Serves as an *example* of a white paper to be submitted by vendors interested in obtaining certification and accreditation (C&A) of a Digital Imaging (DI) System, Teleradiology (TR), or Picture Archiving Communications System (PACS); sole purpose of data submission is for the government to assess a vendor's ability to meet "C2" and network security requirements
 - C2 is an old term, and while it is rooted in the "Orange Book" and the Trusted Computer Base (TCB) requirements of past DOD guidance (i.e. DOD 5200-28), it still denotes the standard that is still sought with respect to a discretionary access control implementation of the system and its interface to the underlying operating system (OS) and the application presentation to the user
 - Document is in an outline format, the substantive data provided within the outline should describe the vendor's product and security features/capabilities as it pertains to the specific application; if underlying operating system (OS) security features are used as a system foundation, the tie-in or link of the application to the underlying OS should be clearly explained
 - Section 5 Trusted Computing Base, speaks directly to the capabilities of the system to meet requirements of a TCB; the vendor's response should answer the "Orange Book Requirement" provided in blue text; copies of *all* user manuals, service manuals, and set-up and configuration manuals shall be required for review by assessment agencies
 - Not all inclusive, vendors must review all relevant references, DOD and Air Force Instructions, manuals and directives to meet the intent of this example outline and white paper format; information will NOT be released to non-government agencies; vendors should ensure answers accurately reflect system capability and requirements completely and concisely
- Security Features Users Guide (SFUG)
 - SFUG is an AF requirement for the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) submission to the Air Force Communication Agency (AFCA); the submission is included as Appendix W in the System Security Authorization Agreement (SSAA) between the Base Communication Agency and the using facility
 - IAW DOD TCB criteria, it is "a single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another."
 - National Computer Security Center Technical Guide to writing an SFUG for a TCB is included in the associated zip file; the OEM is encouraged to use this for the development of this requirement (ref NCSC-TG-026, Guidelines for Writing the SFUG)
- Trusted Facility Manual (TFM)
 - IAW DOD TCB criterion, a TFM is one of the documents necessary to satisfy the requirements of any class of a TCB; the TFM is directed towards the administrators of an installation that uses, or intends to install a TCB system; TFM is an AF requirement for the DITSCAP submission to the AFCA; the submission is included as Appendix V in the SSAA between the Base Communication Agency and the using facility
 - The goal of the TFM is to provide detailed, accurate information on how to administer a TCB and provide the following security capabilities for the system administrator (SA); (1) Configure and install a specific secure system; (2) Operate the system in a secure manner; (3) Make effective use of the system privileges and protection mechanisms to control access to

administrative functions and databases; (4) Avoid pitfalls and improper use of the administrative functions that would compromise the Trusted Computing Base (TCB) and user security

-- National Computer Security Center Technical Guide to writing a TFM for a TCB is included in the associated zip file; the OEM is encouraged to use this for the development of this requirement (ref NCSC-TG-016, Guidelines for Writing the TFM)

- CITPO Interface Request 2002

-- CHCS (Composite Healthcare Computer System) is the DOD Healthcare Information System (HIS); a DOD Program Management Office (PMO), the Clinical Information Technology Program Office (CITPO), centrally manages this system

-- The request package serves as a guidance document and formal request required by the CITPO for any system to develop an interface, or connect to an approved interface, if the vendor does not already have CITPO permission for interconnection

-- This requirement is outside of the AF CoN requirements; all requirements imposed under this document are a requirement for interfacing to the DOD HIS, and its associated modules (e.g. laboratory, Radiology); only needed for HIS interface approval

SUMMARY

The four documents referenced in this paper are required as inputs for the DITSCAP and ultimately to achieve an AF CoN and to interface to the DOD HIS; full, complete, concise responses, and all required vendor documentation up front can enhance the speed of meeting the imposed network security requirements; requirements support the desired AF CoN end-state. The final determination is based on an overall risk assessment as documented in the DITSCAP SSAA after complete system testing for system certification and risk acceptance by the Functional Designated Approval Authority (DAA). The DAA signature is the formal accreditation of the system. The DITSAP serves as an input of the subject system to the Air Force Communication Agency (AFCA) from the Program Management Office (PMO) for AF CoN consideration; the Air Force Chief Information Officer (CIO) awards an AF CoN based on the recommendation of the two assessment agencies