



DoD IA/C&A CHALLENGES FACING MEDICAL DEVICE AND PRODUCT VENDORS

A White Paper

January 2011

This page intentionally left blank.

Table of Contents

1	<u>INTRODUCTION.....</u>	<u>2</u>
1.1	Reciprocity	2
1.2	DIACAP Implementation Delays.....	2
1.3	Business to Business (B2B) Gateway	3
1.4	Facility Clearance/Facility Security Officer (FSO)	3
1.5	Accreditation Maintenance	3
1.6	C&A Transformation	3
2	<u>CONCLUSION</u>	<u>4</u>

1 INTRODUCTION

The DoD Information Assurance (IA) compliance landscape is changing at a very rapid pace with no indication of slowing in the near future, in fact quite the opposite given the Certification and Accreditation (C&A) Transformation expected within the next one-two years. Standardization and enterprise level insight are the two primary fuels for the DoD changing landscape as well as placing responsibility on the vendor to meet security requirements, whereas historically this responsibility primarily fell upon the Government. Currently the areas posing the greatest challenges to medical device/system vendors are as follows:

- Reciprocity
- DIACAP Implementation Delays
- Business to Business (B2B) Gateway
- Facility Clearance/Facility Security Officer (FSO)
- Accreditation Maintenance
- C&A Transformation

1.1 RECIPROCITY

Reciprocity is the reuse of an accreditation from one DoD Component to another. Although a DoD Reciprocity Memo was signed by the Principal Approving Authorities (PAAs) in July 2009, it is not yet the case that reciprocity is exercised as expected at this point. The intent of the memo was to support acceptance of an accreditation from one Component to another, thereby decreasing the time to field capabilities, rework in documentation, testing, etc. The challenge is that vendors may still be required to process individual accreditation packages per each Component approval chain. Reuse of many DIACAP artifacts is common; however additional certification testing is typically required, thereby significantly delaying the accreditation process for the second Component. Vendors are challenged by the cost of such activities as well as having to learn the nuances in the DIACAP implementation of the new Component.

1.2 DIACAP IMPLEMENTATION DELAYS

Although the DIACAP has been standardized at the Department level, it is the case that each Component has nuances to the process. The first challenge to vendors is determining the implementation specifics pertaining to the Component with which they are working. Obtaining accreditation, e.g., Authority to Operate (ATO) is not a rapid process in that it only takes a couple of weeks or so, in fact accreditation is a lengthy process initially and then maintaining that accreditation is required for the duration of the system's lifecycle. This raises the second challenge which centers around turnover relative to the approval chain support personnel (typically contractors). A knowledgeable DIACAP team lead representing the vendor is a good safeguard against such occurrences having a significant impact on program timelines.

1.3 BUSINESS TO BUSINESS (B2B) GATEWAY

Although the B2B Gateway process is not new, it is not formally documented in an easy to follow manner. Further, during the building of the solution, questions arise as to the vendor side technical implementation requirements. The Medical Device STIG contains guidance, however little standardization exists relative to the validation of and subsequent reporting for technical specifics on the vendor side, e.g., behind the DISA configured VPN device/router. The good news for vendors is that the B2B process does not have differences depending upon sponsoring Component. TIMPO (now renamed to MCIS) is the point of contact for all B2B Gateway implementations regardless of Component; DISA is the approval authority.

1.4 FACILITY CLEARANCE/FACILITY SECURITY OFFICER (FSO)

Historically, sponsoring DoD Components typically processed the background check or clearance requests for authorized vendor employees on behalf of the vendors with which they are conducting business. This has become a significant burden on the sponsoring entity's FSO and further is not the intent of DSS or OPM. As a result, the requirement to obtain a facility clearance and thus establish their own FSO has been levied on DoD medical vendors. Obtaining a facility clearance requires a contract with an appropriate DD254, identification and clearing of Key Management Personnel (KMP), and adherence to the NISPOM, among other requirements. The challenge begins with the identification of the appropriate Defense Security Services (DSS) Representative which is aligned to the vendor's physical location vs. the sponsoring Agency. Slight process-nuances exist based on DSS Field Office which complicates the situation. Obtaining a facility clearance is not a quick process, therefore the onus falls on the vendor to identify a short term solution for the processing of employees for background checks and/or clearance investigations.

1.5 ACCREDITATION MAINTENANCE

Accreditation does not end when an ATO is obtained; accreditation is an on-going activity requiring consistent and regular IA activities to include configuration management, patch/IAVM compliance, reporting of continuous monitoring, etc. The challenges for vendors are determining the requirements, figuring out how to implement a patch management (IAVM) plan, and accurately reporting on C&A compliance in the appropriate manner, e.g., via entry in tracking management system, notification to Program Office, etc. Another major challenge is ensuring an open channel through which changing and new requirements can be communicated to the vendor for implementation and adherence purposes.

1.6 C&A TRANSFORMATION

The C&A Transformation is a movement across the entire Federal Government to establish a standardized C&A process, requirements set, and validation techniques for Federal Civilian

Agencies, DoD, and the Intelligence Community. The process and requirements will be based upon the National Institute of Standards and Technology (NIST) Special Publication (SP) series, e.g., 800-53/53A. While this may not be an immediate challenge for the DoD medical device/system vendors, this is a change that will affect the entire DoD as C&A (process and requirements) will change significantly. Some Components, e.g., DISA, have begun to integrate NIST templates, etc., into their existing C&A process.

2 CONCLUSION

The above list is only a subset of the many IA/C&A challenges facing medical device/system vendors relative to DoD compliance. Additional, more specific challenges exist, some are Component specific, e.g., the Army Certificate of Networthiness (CON) process, and others are situation specific, e.g., approved use of foreign nationals in system support/development.

Please contact Lunarline with any questions and/or requests for support.