



FINAL REVIEW MEMORANDUM

Date Received: May 12, 2015
June 12, 2015
December 13, 2016
March 20, 2017
May 18, 2017
May 23, 2017
October 10, 2017
November 20, 2017
December 04, 2017
December 19, 2017

Reviewer: Lisa Simone, Ph.D., PRB/ DETTD

Through: David A. Leiby, Ph.D., Chief, PRB/DETTD

To: Robert Duncan, Ph.D., Scientific Lead, LEP/DETTD
RPM: Iliana Valencia, RPM, RPMS/OBRR

Product: *Babesia microti* Arrayed Fluorescence Immunoassay (AFIA)
Sponsor/Applicant: Oxford Immunotec, Inc. (was: IMUGEN)
Submission Type: Biologics License Application
STN: 125589/0
Scientific Disciplines Reviewed: Software and Instrumentation

Recommendation: Approvable.

Note to Lead Reviewer/Scientific Lead: A final comment should be sent to the applicant as described in Reviewer Notes and Recommendations, Section 5d) Reviewer Recommendation.

Table of Contents

1	Purpose, Intended Use and Regulatory History.....	2
2	Final Review Summary for Software and Instrumentation	3
3	Device Description Overview	5
4	Review: Original Submission and Significant Supplements	7
5	Software and Instrumentation Documentation Status and Adequacy.....	11
6	Reviewer Notes and Recommendations.....	23
7	Appendix 1: Sponsor/Applicant Interactions and Communications.....	25
8	Appendix 2: Device Description Details	54

1 Purpose, Intended Use and Regulatory History

Purpose

The applicant submitted two biologic license applications (BLAs) for the screening of blood donors for evidence of *B. microti*. These include:

- *Babesia microti* AFIA (indirect fluorescent antibody) (this submission, BL125588)
- *Babesia microti* NAT (nucleic acid test by real time polymerase chain reaction) (BL 125589)

The same software is common for these two BLAs, although some software functionality is unique to the NAT Intended Use. As a result, there is significant overlap in the review of these two submissions, which were reviewed concurrently.

Intended use / Indications for use

The Imugen *Babesia microti* Arrayed Fluorescence Immunoassay (AFIA) is intended for qualitative detection of antibodies to *B. microti* in human plasma (EDTA anti-coagulated) samples. This test is intended for use as a donor screening test to detect antibodies to *B. microti* in plasma samples from individual human donors, including volunteer donors of whole blood and blood components, as well as other living donors. It is also intended for use to screen organ and tissue donors when specimens are obtained while the donor's heart is still beating.

This test is not intended for use on specimens from cadaveric (non-heart beating) donors.

This test is not intended for use on samples of cord blood.

This test is not intended for use as an aid in the diagnosis of *B. microti* infection.

Past and Concurrent Submissions

- IND 14532 (and its related amendments) submitted for clinical studies to support the Babesia NAT and AFIA assays – received 02/21/2012
- BL 125588 *Babesia microti* Nucleic Acid Test (NAT) – received 05/12/2015
- BQ 170068: Submission Issue Meeting July 6, 2017 for inspectional issues and software
- BQ 170083: Submission Issue Meeting Request August 4, 2017 for software issues

Interactions for current submission (communication history)

- 05/12/15: Original submission received
- 06/12/17: Amendment 1: Summary information for original submission

- 09/29/15: CR letter issued, including for original, generic software deficiencies rather than actual software deficiencies
- 02/10/16: Face to Face, including question about software deficiencies
- 12/13/16: Amendment 12: Resubmission received with CR issue responses
- 02/24/17: IR email sent, with relevant 9/29/15 software questions not sent in original CR and new issues resulting from CR responses (Note: five common questions accidentally omitted in SL memo, but were included in NAT IR dated 02/20/17)
- 03/20/17: Amendment 13: IR response received for 02/24/17 issues
- 04/14/17: IR email sent for software issues from 03/20/17 response
- 04/20/17: Telecon for software and cybersecurity issues
- 05/18/17: Amendment 21: Risk documentation to more closely align with ISO 14971
- 05/18/17: Emailed advice in response to risk documentation provided 5/18/17
- 05/23/17: Amendment 22: Status update on software with documentation
- 06/13/17: CR letter issued, inspectional issues and major software issues
- 07/17/17: Submission Issue Meeting Request for feedback on software; FDA written response sent 08/04/17. Meeting request cancelled by the applicant on receipt of FDA responses.
- 10/10/17: Amendment 27: Complete Response received
- 11/09/17: IR email sent for software
- 11/20/17: Amendment 29: IR response received
- 11/30/17: IR email sent for software; AFIA Risk Assessment spreadsheet is missing
- 12/04/17: Amendment 31: IR response received
- 12/5/17: Telecon to discuss AFIA risk assessment document received 12/04/17
- 12/19/17: Amendment 33: IR response received

2 Final Review Summary for Software and Instrumentation

*The following is a **final** review summary for software and instrumentation in original submissions and significant supplements that can be cut-and-pasted into final documentation such as SBRAs/SSEDs.*

The following is a summary overview of software, instrumentation and risk management information provided to support a reasonable assurance that the device is safe and effective for its intended uses and conditions of use.

Versioning: Software: (b) (4) Build 1.0.5.5 (not for commercial release). Hardware: (b) (4) workstations in client/server configuration for processing, AFIA testing, and reporting; all running supported versions of Windows (Windows (b) (4)) and Windows Server (b) (4). During the review period, the software was upgraded from Build 1.0.5.4 to correct an unresolved NAT-related anomaly and to migrate a database server from an unsupported version of Windows.

Device Description: The system supporting the NAT and AFIA assays is comprised of an RNA/DNA extraction system, real time PCR system, custom (b) (4) software, refrigerator, freezer and other sample handling tools. The custom software called (b) (4) is used to collect and report data for blood donor sample testing within the Oxford facility. It does not control laboratory equipment, but facilitates collection of data, stores batch and sample data and test results where the data is acquired through barcode scanning, touch-screen and keyboard entry, and electronic file import. Sample results are electronically transmitted via email or FTP to the submitting entity.

Risk Management: Risk processes and associated artifacts were significantly updated and refined for better alignment with ISO 14971 “Medical devices – application of risk management to medical devices” and harmonized between the NAT and AFIA assays and submissions. Use of the new process allowed the applicant to capture significantly more risks and mitigations at a level of detail appropriate to ensure that proposed risk control measures could be appropriately verified. Reanalysis of risk across the system led to several new and changed requirements and specifications, and the development of corresponding testing.

The initial hazard analysis included 12 incompletely-developed risks. The final risk assessment included 3 Excel spreadsheets with a total of 352 risks fully characterized with explicit hazards, relevance to the software or product, cause, sequence of events, outcome, hazardous situation, premitigation and postmitigation assessment of risk, controls measures, and the type of mitigation employed to reduce the risks to acceptable levels. The three risk documents address (b) (4) manufacturing and assay risks, cybersecurity risks, and AFIA processing related risks.

Risk analysis revealed 18 (b) (4) manufacturing and assay risks, 58 AFIA processing-related risks, and 43 cybersecurity risks with a premitigation assessment of “Not Acceptable” related to alteration or deletion of stored data (including results), and reporting incorrect negative results. These are caused by issues with system access, performance, results reporting, interface and audit functionality. AFIA-processing causes include batch inhomogeneity and inconsistency, imprecise measurements, specimen identification errors, stability problems, problems preparing samples, use error, uncertainties with cutoffs and interfering factors, bio-contamination, incorrect formulation, degradation, inadequate labeling, inadequate instructions, inadequate hazard warnings, incompatibilities with consumables and other devices, and misrepresentation of results. Primary hazardous situations include: 1) release of an infected unit for use in transfusion, 2) a unit inappropriately discarded, and 3) a unit delayed prior to transfusion or discarded, reducing the donor blood pool. All risks have been reduced “as far as possible” though multiple mitigations, and the applicant has provided a further Risk/Benefit analysis to support that the overall residual risks are acceptable. Overall, the applicant has done an impressive job establishing processes which should allow them to ensure that existing risks remain controlled, and that new risks can be easily assessed and mitigated.

Unresolved Anomalies: No unresolved anomalies have been reported.

Testing: Verification and validation testing initially focused on Installation Qualification (IQ), Performance Qualification (PQ), and Operational Qualification (OQ) testing of the (b) (4) software. Because this black box testing cannot exercise all pathways through software and did not include verification of the many new risk mitigations, additional unit and integration testing was developed and performed. This focused on higher level risks associated with errors and unexpected conditions related to user inputs and workflow, database integrity and performance, and cybersecurity mitigations related to data loss or corruption, improper access and improper software patching. All new testing was successfully completed.

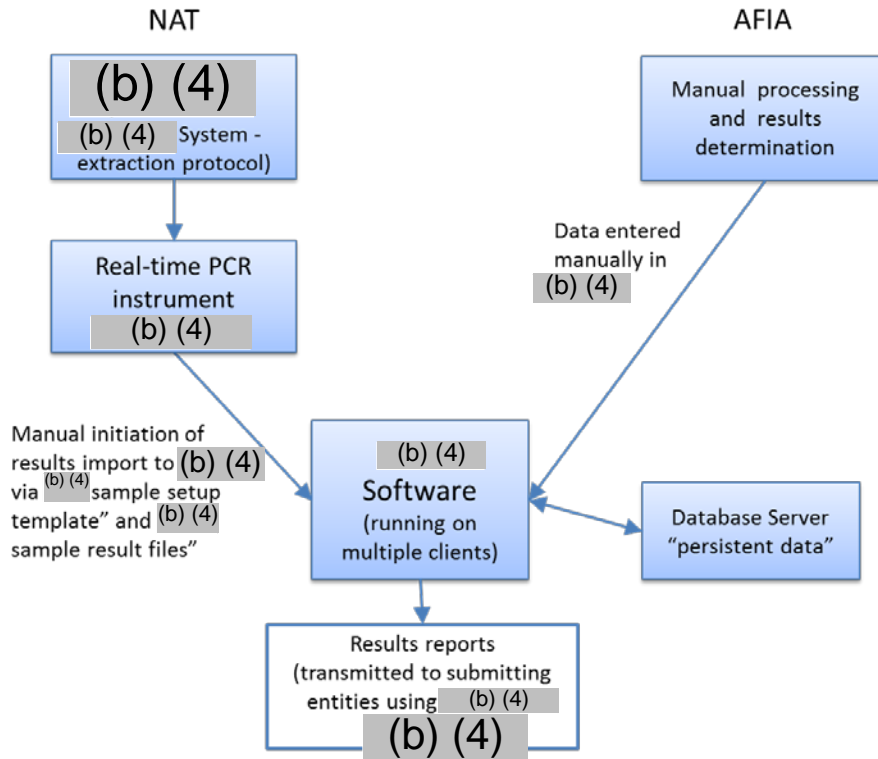
Development Management: The software development activities included establishing detailed software requirements, linking requirements with associate verification tests, verification and validation testing, defect tracking, configuration management and maintenance activities to ensure the software conforms to user needs and intended uses.

3 Device Description Overview

The system supporting the NAT and AFIA assays is comprised of an RNA/DNA extraction system, real time PCR system, custom (b) (4) software, refrigerator, freezer and other sample handling tools. Custom software called the (b) (4) is used to collect and report data for blood donor sample testing within the Oxford facility.

The figure below illustrates the relationship between the NAT and AFIA assay processing paths and the combined role the that (b) (4) software plays. Both the NAT and AFIA assays require a number of manual operations before data is inputted into the (b) (4) software. The AFIA processing is completely manual. As a result, the “device” under review is actually a combination of the manual and automated processing, and the use of the (b) (4) software to manage the processes.

The (b) (4) software does not control laboratory equipment, but facilitates collection of data, stores batch and sample data and test results where the data is acquired through barcode scanning, touch-screen and keyboard entry, and electronic file import. Sample results are electronically transmitted via email or FTP to the submitting entity.



The software has four primary functional roles and two secondary functional roles. These are listed and described below:

Primary Functional Roles:

1. Process: provides data entry screens to create new batches, add samples to a batch, review and close batches and print barcode labels.
2. IFA: provides data entry screens to create IFA test runs, add slide(s) to a test run, add sample(s) to a slide, and to enter IFA test results for each sample.
3. PCR: provides a screen to import the sample template setup from the (b) (4) (b) (4) real-time PCR system, and (b) (4) sample result files.
4. Report: provides screen(s) to create two types of reports: Proof Copy and Final sample results.

Secondary Functional Roles: (Note: these are not required to perform essential services for data collection and reporting, and are restricted to users with elevated privileges):

1. Audit: provides read-only access to data for a specific sample.
2. Admin: provides limited data management functionality.

Additional information about the device infrastructure can be found in Appendix 2: Device Description Details.

4 Review: Original Submission and Significant Supplements

Scope

All documentation related to software and instrumentation was reviewed. See section 5, “Software and Instrumentation Documentation Status and Adequacy” for specific documents reviewed.

Review

Table 1 below reflects the final status of the review with respect to specific documentation outlined in Agency’s software guidance document (Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, available at <http://www.fda.gov/RegulatoryInformation/Guidances/ucm089543.htm>). Please see section 5, “Software and Instrumentation Documentation Status and Adequacy” for a detailed review of each type of documentation.

Table 1. Summary of Software Documentation

	Present	Missing	Adequate (Yes/No/ Assessment Incomplete)
1. Level of Concern:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Yes
2. Software Description:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Yes
3. Device Hazard Analysis:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Yes
4. Software Requirements Specifications:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Yes
5. Architecture Design Chart:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Yes
6. Software Design Specifications:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Yes
7. Traceability Analysis/Matrix:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Yes
8. Software Development Environment:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Yes
9. Verification & Validation Testing:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Yes
10. Revision Level History:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Yes
11. Unresolved anomalies:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Yes
12. Cybersecurity:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Yes
	YES	NO	
EMC Review Required?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Due to the depth of the interactive discussions, please also refer to the Interactive Questions in Appendix 1: Sponsor/Applicant Interactions and Communications for the detailed issues and resolutions.

Versioning: During the course of this review, the applicant was requested to correct an unresolved anomaly related to the NAT assay and update the software version from Build 1.0.5.4 to Build 1.0.5.5. Updated design control documentation was provided to support the upgrade. See Interactive Question #12. This was coupled with migration of a database server from an unsupported version of Windows, as discussed in Interactive Question #13.

Requirements, Architecture and Specifications, Traceability Matrix: Initial design control documents were extremely limited in detail. Final documentation is much more comprehensive, and allows traceability between design inputs and design outputs and reference to risk documentation. The requirements are significantly expanded to more adequately reflect the known requirements of the system, and the architecture document more clearly includes the components of the system and boundaries with the business IT infrastructure and outside world. Performance requirements for the (b) (4) software, hardware, and IT infrastructure were alternately included and removed, and finally restored and optimized after the applicant came to understand that the infrastructure performance is associated with identified risks.

Specifications were initially sparse and untestable but upgraded to include significant detail for the individual process workflows and screenshots depicting user interactions and error checking functionality. The specifications are not traditional statements with testable metrics because the specifications were reverse-engineered after the (b) (4) software was written. This is adequate for this submission, although the applicant may be challenged to add future specifications without significant changes to the document. The (b) (4) database server was upgraded at FDA's request from an unsupported version of Windows (Windows Server (b) (4) to Windows (b) (4). See Interactive Questions #2, 7, 9, 11 (requirements), #2, 3 and 10 (architecture) and #4 (specifications). The updated traceability matrix appropriately links requirements, specifications, risk IDs and corresponding test cases. See Interactive Questions #1 and 5.

Hazard analysis and risk management: The applicant originally had no risk management process. Documentation for the original submission was developed as part of a "retrospective design review." Although some initial documentation referenced FDA's guidance, "Q9 Quality Risk Management," the applicant ultimately designed a risk management process and associated documentation to harmonize the NAT and AFIA risk assessments and to better align with ISO 14971 "Medical devices – application of risk management to medical devices" rather than with ICH Q9. This is acceptable.

The initial hazard analysis included 12 incompletely-developed risks. The final risk documentation contained three spreadsheets of risk information. The final (b) (4) manufacturing and assay risk assessment included an Excel spreadsheet with 127 risks with explicit hazards, relevance to the software, relevant component, cause, outcome, hazardous situation, premitigation and postmitigation assessment of risk, controls measures, and type of mitigation. A separate spreadsheet included 60 cybersecurity related risks. Primary risks result from assay failure, false negative results, false positive results, and cybersecurity hazards which

have the possibility of allowing any of the above. These were associated with unauthorized access to various parts of the system, source code or database that might allow loss or corruption of data, improperly patched software or firewalls or infected files, add-ons and logins. Primary hazardous situations include release of an infected unit for use in transfusion, a unit inappropriately discarded, and a unit delayed prior to transfusion or discarded, reducing donor blood pool. A separate AFIA risk assessment included 165 risks related to manual assay processing.

Risk analysis revealed 18 (b) (4)-related manufacturing and assay risks, 58 AFIA processing-related risks, and 43 cybersecurity risks that were considered “Not Acceptable” prior to mitigation. The (b) (4) and cybersecurity “Not Acceptable” risks were associated with unauthorized access to various parts of the system, source code or database that might allow loss or corruption of data, improperly patched software or firewalls or infected files, add-ons and logins. Other “Not Acceptable” risks were associated with alteration of data caused by inappropriate access to the system, operator error, incorrect information sent to the customer, sample ID tracking and data traceability issues. The AFIA “Not Acceptable” risks were associated with batch inhomogeneity and inconsistency, imprecise measurements, specimen identification errors, stability problems, problems preparing samples, use error, uncertainties with cutoffs and interfering factors, bio-contamination, incorrect formulation, degradation, inadequate labeling, inadequate instructions, inadequate hazard warnings, incompatibilities with consumables and other devices, and misrepresentation of results. All risks were reduced to at least “As Far As Possible.”

The final risk assessment is significantly more comprehensive than in the original submission, with multiple causes for the same risks individually captured and assessed. The assessments appear to capture the risks and mitigations in the system, and are of an appropriate level of detail to ensure risk control measures can be appropriately verified.

The significant improvement in the applicant’s final risk documentation was possible because the risk management procedure was designed to align with ISO 14971 “Medical devices – application of risk management to medical devices.” A detailed procedure for risk analysis was provided, including how information is added to the risk tables. (b) (4) methods have been added for consideration in the early stages of product design. Risk processes are integrated into the larger quality system, and the relationship to premarket and postmarket activities is outlined. The specifics of the improved process are discussed in Section 5 for “Device Hazard Analysis.”

Overall, the applicant has done an impressive job establishing processes which should allow them to ensure that existing risks remain controlled, and that new risks can be easily assessed and mitigated. See Interactive Questions #1, 7, 8, 9, and 11 related to risk management.

Verification and validation testing: The applicant supplemented originally-performed Installation Qualification (IQ), Performance Qualification (PQ), and Operational Qualification (OQ) testing with some additional unit, integration and system testing as outlined in FDA’s

premarket guidance document. However, because the specifications were developed by reverse engineering the software, they were not constructed in a manner to facilitate true verification testing such as unit level testing. See Interactive Question #5.

At this point, it appears that the benefits of getting this test to market outweigh the risks of forcing the applicant to undergo the lengthy process of fully reverse engineering the design specifications and testing schemes to ensure verification has been performed completely. Instead, focus was placed on developing an adequate risk process and using that to guide the review to ensure testing would adequately cover the identified risks. The applicant developed additional testing for error conditions and unexpected conditions related to user inputs (see Interactive Question #11), testing for database integrity and performance (see Interactive Question #2), and testing of cybersecurity mitigations for unacceptable risks (see Interactive Question #10). The original five test documents were supplemented with an additional 14 testing documents.

Cybersecurity: The initial submission contained no references to cybersecurity, despite the software running on several individual computers and servers that are shared with the applicant's business IT infrastructure. The IT business network is not completely isolated from the computers used to perform the assays, which exposes the (b) (4) software and servers to additional cybersecurity risks. To address this, a new cybersecurity risk assessment was performed and cybersecurity testing protocols developed and completed. The applicant developed new processes to ensure several common mitigations for cybersecurity hazards have been implemented. A new "Business Continuity and Disaster Recovery Plan" was created and the "Information Technology Security Policy" was significantly updated. See Interactive Questions #5, 6 and 10.

Other: Several deficiencies were related to unresolved anomalies, the final version of software to be used, and various features.

- In contrast to original documentation, the applicant confirmed the software will not be recompiled for commercial release, as discussed in Interactive Question #12.
- Transmission of results data between the laboratory and blood establishment facilities is discussed in Interactive Question #7.
- One server was running an unsupported version of Windows, which was upgraded and validated during the course of this review, as discussed in Interactive Question #10.

For additional information and details on these areas, see the appropriate subsections in the Section: Software and Instrumentation Documentation Status and Adequacy.

Labeling

Because this submission represents a service rather than a device that is marketed and sold, labeling requirements are reduced. Screenshots of error detection and recovery related to risk mitigations implemented in labeling were reviewed. No other aspect of labeling review was performed.

5 Software and Instrumentation Documentation Status and Adequacy

Documentation Reviewed

The applicant provided the following documentation, in an attempt to fulfill specific documentation outlined in Agency's software guidance document. The design control documentation was submitted three separate times:

- 1) In the original submission, in the Table of Contents (062_Attachment 4-5-1 (b) (4) Software Table of Contents.pdf) the applicant described the documentation submitted for software. See folder "VOL_004_VOL_004_Chemistry_Manufac."
- 2) In the amendment received December 13, 2016, the applicant provided updates for nearly all design documentation. Responses to software and instrumentation questions begin on page 35 of the response document (001_AFIA Response to AI p 1 to 260.pdf).
- 3) Finally, in the CR response received October 10, 2017, the applicant provided significantly updated documentation, and provided the (b) (4) Submissions Table (050_Attachment-13.3_(b) (4) submissions table.pdf) that lists all documents ever provided for this submission related to software and instrumentation, when each was provided, and which are obsolete. **This table should be used to ensure correct documents are referenced because a majority are obsolete.**

1. Level of Concern (LOC): Acceptable

In the original submission, in the Level of Concern document (063_Attachment 4-5-2 Imugen (b) (4) Level of Concern Determination.pdf) the applicant stated that the Level of Concern is Major. This is acceptable.

2. Software /Firmware Description: Acceptable

In the original submission, in the document "(b) (4)", Software Description" (064_Attachment 4-5-3 Imugen(b) (4) software description_20150324.pdf) the applicant stated that the (b) (4) is designed to collect and report data for blood donor sample testing within the Oxford (was: Imugen) facility. (b) (4) is designed to be a simple (b) (4) and, as such, does not control laboratory instruments. (b) (4) also does not perform any algorithmic computation of instrument data to produce results.

The applicant further stated that (b) (4) is a client/server application that provides graphical user interface screens for laboratory technicians to process batches of samples sent by submitting

entities to Oxford. The software is used to collect and store batch and sample data and test result data for the samples under test. Data entry is accomplished by barcode scanning, touch-screen and keyboard entry, and electronic file import. When testing and data collection is complete, laboratory managers use the software to produce reports of sample results which are electronically transmitted to the submitting entity. Data is persisted until testing is complete and a final sample report is produced. The reports associated with samples are reported back to the submitting entity.

The software has four primary functional roles and two secondary functional roles. These are listed and described below:

Primary Functional Roles:

1. Process: provides data entry screens to create new batches, add samples to a batch, review and close batches and print barcode labels.
2. IFA: provides data entry screens to create IFA test runs, add slide(s) to a test run, add sample(s) to a slide, and to enter IFA test results for each sample.
3. PCR: provides a screen to import the sample template setup from the (b) (4) (b) (4) real-time PCR system, and (b) (4) sample result files.
4. Report: provides screen(s) to create two types of reports: Proof Copy and Final sample results.

Secondary Functional Roles: (Note: these are not required to perform essential services for data collection and reporting, and are restricted to users with elevated privileges):

1. Audit: provides read-only access to data for a specific sample.
2. Admin: provides limited data management functionality.

On page 862 of the Software Description document, the applicant listed the hardware requirements, programming language(s) used, and off-the-shelf software required for software development.

3. Device (including software) Hazard Analysis (HA): Acceptable

In the original submission, the applicant provided a hazard document (065_Attachment 4-5-4 (b) (4) Hazard Analysis.pdf) for the (b) (4) which lists 12 potential hazards with estimated severity, hazard mitigation and a severity estimation after mitigation. No potential causes are listed. Mitigations are of too high a level to ensure they can reduce risk to acceptable levels. During a retrospective design review of AFIA, a retrospective design risk assessment was performed (115_Attachment 4-9-2-5 LAB-DSGN-5.pdf), although at the time this was performed, Imugen stated that it had not established a formal Risk Management SOP (pg. 3, 112_Attachment 4-9-2-2 LAB-DSGN-2.pdf). No process had been developed although ICH Q9 “Quality Risk Management” was referenced and a “typical” risk management process presented in Figure 1.

In the original submission, the applicant did not provide an enumerated description of the hazards (including clinical hazards) presented by this device, the causes and severity of the hazards, the method of control of the hazards and the testing done to verify the correct implementation of that method of control, and any residual hazards. Deficiencies were written for the Complete Response sent December 2015, which started several interactions where the applicant reassessed their entire risk management methodology and developed new processes. See Appendix 1: Sponsor/Applicant Interactions and Communications, Interactive Questions #1, 7, 8, 9 and 11 for resolution of deficiencies related to hazard analysis and risk management.

Additional documentation was provided in the following, where the documentation was significantly updated.

- Complete Response received December 13, 2016
- Amendment received March 20, 2017
- Complete Response October 10, 2017
- Amendment received December 4, 2017
- Amendment received December 19, 2017

After the resolution of all deficiencies, the applicant implemented a redesigned and substantially improved risk management procedure, LAB-QA-62 (BL 125589, 005_Attachment-5.1_LAB-QA-62_DocDetails.pdf) that is aligned with ISO 14971 “Medical devices – application of risk management to medical devices.” The procedure was “activated” on December 18, 2017 “for all products and services manufactured and operated by Oxford Immunotec, Inc.” A “Memo on Risk Management” (LAB-MEM-38) was initially provided during interactive review to describe the thinking before the final procedure was produced and finalized. The following improvements were made:

- Removed economic considerations from assessment of risk
- Risk-benefit analysis now required for all risks, not just Unacceptable or ALARP risks
- Clarification of process risk management, including additional mitigation review
- Added use of (b) (4) as appropriate, at the commencement of product design
- Added (b) (4) methods (b) (4) for use in early design stages
- Updated terminology to align with ISO 14971
- Patient harm added to assessments, rather than limiting the analysis to erroneous patient sample results
- Risk management file is now updated during all phases of the design and development process
- Detailed flowchart created to show pre and post market risk management processes (Figure 1, page 7)
- A detailed procedure for risk analysis is provided, including how the information is entered into the risk management table. Product risk assessment is based on an FMEA. For blood donor screening, a more detailed approach is required. Multiple risk controls are required to reduce the risk as low as possible; each risk control must be assessed and

scored individually to assess residual risk. Risk acceptability is different for donor screening tests and IVDs intended to aid in diagnosis.

- Full integration of postmarket information into the risk processes
- Documentation storage requirements and mitigation review

Final risk documentation is included in the following documents:

- Cybersecurity: 048_Attachment-12.2_DOC-RSK-9_Cybersecurity Risk Assessment.xlsx
- (b) (4) software: 031_Attachment-8.9_IT-CSV-PDF-41(b) (4) Risk Analysis Rev. 1.4.xlsx
- AFIA Risk Assessment: 002_Attachment-2_LAB-DSGN-5.xlsm
- Risk Management Process: 001_Attachment-1_LAB-QA-62_DocDetails.pdf
- Overall Risk/Benefit and Residual Risk Summary: 003_Attachment-3_Risk Benefit Analysis and Overall Residual Risk Summary.pdf

The AFIA assay has a separate, updated risk assessment (002_Attachment-2_LAB-DSGN-5.xlsm) that lists 47 potential hazard IDs and 165 associated risks. Each of these is expanded into individual line items totaling 796 sequential IDs to capture the various sequences of events that may result in harm(s) and individual mitigations that collectively reduce the risk to acceptable levels. The spreadsheet contains a number of grey “summary” rows that are used to summarize the contributions of several mitigations presented in previous rows. An assessment of residual risk is provided. The redesigned risk management procedure, LAB-QA-62, describes how to assess the overall risk for multiple mitigations. 58 of the 165 risks were associated with a pre-mitigation risk of “Not Acceptable” for hazards including: batch inhomogeneity and inconsistency, imprecise measurements, specimen identification errors, stability problems, problems preparing samples, use error, uncertainties with cutoffs and interfering factors, bio-contamination, incorrect formulation, degradation, inadequate labeling, inadequate instructions, inadequate hazard warnings, incompatibilities with consumables and other devices, and misrepresentation of results. All risks were reduced to acceptable levels.

During the course of this review, the applicant created a “Business Continuity and Disaster Recovery Plan” (Attachment_20.1-DOC-POL-1.pdf) that focuses on business risk and includes data backup and recovery plans. The applicant also provided a substantial update to the “Information Technology Security Policy” (Attachment_20.2-IT-SEC-POL-01&DocDetails.pdf) that includes policies for accounts management, password management, encryption, data security, and software patches and updates, including antivirus updates.

In summary, risk management is not easy, and there is no single accepted way to perform an adequate assessment. Some of the terminology and claims could be better implemented, although overall, the applicant appears to have identified the major hazards and implemented reasonable mitigations for the associated risks.

In the initial hazard analysis, each of 12 potential hazards was associated with a severity estimate, a hazard mitigation, and a severity estimate after mitigation. The applicant now recognizes that severity generally does not change with mitigation, and that risk is the

combination of severity of harm, and probability of occurrence of harm. The final risk assessment is implemented in Excel with automatic calculations, and adds hazards associated with cybersecurity, manual operations, and software issues that could lead to incorrect results. The final risk tables include a wealth of columns for premitigation and postmitigation assessment of risk, the relevance to software, countermeasures to take, mitigation type, and the assay to which the risk applies. The applicant's enhanced risk processes were used to identify and mitigate 127 risks related to the software and assay performance, 60 risks related to cybersecurity considerations, and 165 risks related to AFIA assay processing.

Risk analysis revealed 18 (b) (4)-related manufacturing and assay risks, 58 AFIA device-related risks, and 43 cybersecurity risks were considered "Not Acceptable" prior to mitigation. The (b) (4) and cybersecurity "Not Acceptable" risks were associated with unauthorized access to various parts of the system, source code or database that might allow loss or corruption of data, improperly patched software or firewalls or infected files, add-ons and logins. Other "Not Acceptable" risks were associated with alteration of data caused by inappropriate access to the system, operator error, incorrect information sent to the customer, sample ID tracking and data traceability issues. The AFIA "Not Acceptable" risks were associated with batch inhomogeneity and inconsistency, imprecise measurements, specimen identification errors, stability problems, problems preparing samples, use error, uncertainties with cutoffs and interfering factors, bio-contamination, incorrect formulation, degradation, inadequate labeling, inadequate instructions, inadequate hazard warnings, incompatibilities with consumables and other devices, and misrepresentation of results. All risks were reduced to "As Far As Possible."

4. Software Requirements Specifications (SRS): Acceptable

In the original submission, the applicant provided the document (b) (4) Software Requirements Specification" (066_Attachment 4-5-5 SRS-(b) (4)_IMUGEN-20150324.pdf) that describe the client/servicer application. The document includes 20 requirements for hardware, interface, software, performance, regulatory, system backup and restore, and other. Most requirements are too high level and do not include testable information. Requirements for workflow processes, boundary conditions and error recovery are missing.

In the original submission, the applicant did not provide a copy of the Software Requirements Specification document, which should clearly document the functional, performance, interface, design and development requirements.

Deficiencies were written for the Complete Response sent December 2015. See Appendix 1: Sponsor/Applicant Interactions and Communications, Interactive Questions #2, 7, 9 and 11 for resolution of deficiencies related to software requirements and supported functionality.

Additional documentation was provided in the following:

- Complete Response received December 13, 2016

- Amendment received March 23, 2017
- Complete Response October 10, 2017

After the resolution of all deficiencies, the applicant provided updated software requirements specifications (023_Attachment-6.3_IT-CSV-IMD14-13-SRS &Doc Details.pdf). The format was updated to align with the risk analysis and traceability matrix, and ensure mitigations are captured.

The performance requirements for the system were optimized, including establishing the boundaries of the assay performance portion of the infrastructure from the IT business portion of the infrastructure. This was necessary because the applicant originally stated that the IT infrastructure was beyond the scope of the (b) (4) software. However, this was found to be incorrect because all of the computers and servers are connected and potentially impact one another. To address some untestable requirements, some were changed and others were added to ensure the infrastructure can support the performance requirements of the (b) (4) software. The applicant hired an “FDA consultant” who reviewed the proposed testing. Updated test plans and risk management information were provided. Additional requirements related to security, restricting access, source code archival, (b) (4) database backup and restoration were also added.

The applicant confirmed that results are sent to clients manually by email in PDF format or as a .csv file via secure FTP. The applicant also confirmed that (b) (4) will not be compiled for commercial release, in contrast to claims in the original submission. The complete documentation package for the final version, Build 1.0.5.5, was provided. See Interactive Question #13 for details.

5. Architecture Design Chart: Acceptable

In the original submission, the applicant did not provide a detailed depiction of functional units and software modules, which may include state diagrams as well as flow charts. Deficiencies were written for the Complete Response sent December 2015. See Appendix 1: Sponsor/Applicant Interactions and Communications, Interactive Questions #2, 3 and 10 for resolution of deficiencies related to the system architecture. A software architecture chart was never provided, although FDA constructed a chart based on submission information, which appears in the Device Description Overview. A hardware architecture chart showing the network connections was provided and is included in Appendix 2: Device Description Details to explore the boundaries of the system for risk purposes.

Additional documentation was provided in the following:

- Complete Response received December 13, 2016
- Amendment received March 23, 2017
- Complete Response October 10, 2017

After the resolution of all deficiencies, the applicant provided an updated architecture document (021_Attachment-6.1_IT-CSV-IMD14-15-AD &Doc Details.pdf) that provides significantly more information about the (b) (4) architecture and database architecture, and a hardware network diagram (Section 2.4.2). Information about each of the components in the system was provided, including operating systems and hardware. The applicant also updated the (b) (4) database server, at FDA's request, from an unsupported version of Windows (Windows Server (b) (4)) to Windows (b) (4). Migration testing documentation was provided. See Interactive Question #10 for details.

6. Software Design Specification (SDS): Acceptable

In the original submission, the applicant provided a software design specification document (067_Attachment 4-5-6 SDS-(b) (4)_IMUGEN-20150323.pdf) for the (b) (4). The document includes the modules of the (b) (4) for Process Role, IFA Role, Report Role, Audit Role, and Admin Role. These each illustrate the control flow among the User, the UI, the Data Model and the Data Storage. The database schema is presented in Figure 1 starting on page 886. Definitions are included in Section 2.4 starting on page 889. All components are described by Field with included Notes and Type.

However, none of the Fields have specified measurable or testable values. There is no traceability from the requirements enumerated in SRS document (066_Attachment 4-5-5 SRS-(b) (4)_IMUGEN-20150324.pdf) to this SDS document to describe how the requirements in the Software Requirements Specifications (SRS) are implemented.

Deficiencies were written for the Complete Response sent December 2015. See Appendix 1: Sponsor/Applicant Interactions and Communications, Interactive Question #4 for resolution of deficiencies related to the software design specifications.

Additional documentation was provided in the following, where the documentation was significantly updated.

- Complete Response received December 13, 2016
- Amendment received March 23, 2017
- Complete Response October 10, 2017

After the resolution of all deficiencies, the applicant provided significantly updated software design specifications (022_Attachment-6.2_IT-CSV-IMD14-14-SDS &Doc Details.pdf) with detailed workflow diagrams for each process role. The specifications are not constructed as traditional specifications with testable metrics, but rather as descriptive statements of functionality with screen shots of the corresponding (b) (4) software illustrating their implementation. This is likely because the SDS was reverse-engineered from the completed software program, rather than developed before the software was written. Through the resolution of deficiencies, error checking was added, including screen shots illustrating the error

checking functionality. Additional information to support testing was added. Specifications for hardware to support the software needs were also added.

7. Traceability: Acceptable

In the original submission, the applicant provided a traceability document (068_Attachment 4-5-7 Imugen (b) (4) Traceability Analysis_04092015.pdf) that includes items for each of 22 high level requirements. “V&V Tests” in the form of references to Installation Qualification tests or Operational/Performance Qualification tests are included and associated hazards are identified. Traceability of requirements and specifications to testing and hazards is not comprehensive. This is due in part to inadequately formulated requirements which are often vague and untestable as written, and use of test cases which are mostly limited to using valid values and workflow actions.

In the original submission, the traceability matrix provides traceability among identified clinical hazards and mitigations, requirements, specifications, and verification and validation testing in an enumerated manor.

Deficiencies were written for the Complete Response sent December 2015. See Appendix 1: Sponsor/Applicant Interactions and Communications, Interactive Question #1 and 5 for resolution of deficiencies related to the traceability.

Additional documentation was provided in the following, where the documentation was significantly updated.

- Complete Response received December 13, 2016
- Amendment received March 23, 2017
- Complete Response October 10, 2017

After the resolution of all deficiencies, the applicant provided a significantly updated traceability matrix (026_Attachment-6.6_IT-CSV-IMD14-16-TM &Doc Details.pdf). The trace table includes headings for Risk ID, SRS Ref #, the actual software requirement language, the SDS #, the Architecture section #, V&V test cases and filenames, and an indication of Pass/Fail for the corresponding test case. The matrix was updated several times to address updates in any of the referenced design control documentation (i.e., requirements, specifications, testing, risk analysis).

8. Software Development Environment Description: Acceptable

In the original submission, the applicant provided the Life Cycle Development Plan (069_Attachment 4-5-8 Imugen (b) (4) Life Cycle Development_04172015.pdf) which included an overview of each software development phase. Four control documents (QA scripts) were listed for quality assurance and four process documents were listed that are stated to describe more formalized design control, change control management and verification and validation

processes. These are shown in the figure below. The applicant stated that these will be used in future versions of (b) (4). This is acceptable.

The following table lists the control documents that were generated during the software development process, along with a description of each document.

- (b) (4) QA Script for January 11, 2013 – Testing QNS processing and resulting of QNS variants (**Attachment 4-5-8-1**)
- (b) (4) QA Script for February 14, 2013 – Testing report functions for Recipient Look-Back and Donor Follow-up (**Attachment 4-5-8-2**)
- (b) (4) QA Script for February 22, 2013 – Change to import PCR templates and results including plate report functions (**Attachment 4-5-8-3**)
- (b) (4) QA Scripts for March 27, 2013 – Testing of IFA slide barcode implementation for slide template creation and result entry (**Attachment 4-5-8-4**)

IMUGEN has since implemented a more formalized process for design control, change control management, and verification and validation to be used for future versions of (b) (4)

- | | | |
|-----------------------|---|---------------------------|
| • IT-FAC-PRO-1 | Computer System Design, Validation and Deployment | Attachment 4-5-8-5 |
| • IT-FAC-PRO-2 | (b) (4) Change Control | Attachment 4-5-8-6 |
| • IT-CSV-IMD14-06-IQ | (b) (4) Installation Qualification | Attachment 4-5-8-7 |
| • IT-CSV-IMD14-07-OPQ | Operational/Performance Qualification | Attachment 4-5-8-8 |

9. Verification and Validation Documentation: Acceptable

In the original submission, in the testing document (083_Attachment 4-5-9 Imugen (b) (4) Verification Validation.pdf) the applicant provided verification and validation information for the (b) (4) software. The scope of these V&V activities is not clear, but appears to include only functional requirements and not performance requirements or any testing of error or abnormal conditions, or testing to ensure risk mitigations successfully reduce risk to acceptable levels.

In the original submission, the applicant did not provide a description of the validation and verification activities at the unit, integration, and system level, which should include the unit, integration and system level test protocols including the pass/fail criteria, and test report, summary and test results.

Deficiencies were written for the Complete Response sent December 2015. See Appendix 1: Sponsor/Applicant Interactions and Communications, Interactive Questions #2, 5, 10 and 11 for resolution of deficiencies related to the verification and validation activities.

Additional documentation was provided in the following, where the documentation was significantly updated.

- Complete Response received December 13, 2016
- Amendment received March 23, 2017
- Complete Response October 10, 2017
- Amendment received November 20, 2017

After the resolution of all deficiencies, the applicant developed and performed several additional test protocols. Several interactions with the applicant focused on the use of Installation Qualification (IQ), Performance Qualification (PQ), and Operational Qualification (OQ) testing rather than more detailed unit testing, integration testing and systems level testing. IQ/PQ/OQ testing is generally black box testing, in that it tests the performance of the completed system. This type of testing often omits the type of white box testing that ensures that all error checking works correctly, that the individual software components meet their specifications and that the interface among components is comprehensive, complete and correct. The applicant was resistant to performing appropriate verification testing for the (b) (4) software, although additional testing related to error conditions and risk mitigations was performed. As described in Interactive Question #5, the testing strategy for Build 1.0.5.5 was revised to reference unit, integration and system level testing, although in most cases, the applicant just mapped existing testing to these labels. Because the specifications were developed by reverse engineering the software, they were not constructed in a manner to facilitate true verification testing such as unit level testing.

At this point, it appears that the benefits of getting this test to market outweigh the risks of forcing the applicant to undergo the lengthy process of fully reverse engineering the design specifications and testing schemes to ensure verification has been performed completely. Instead, focus was placed on developing an adequate risk process and using that to guide the review to ensure testing would adequately cover the identified risks. The applicant developed additional testing for error conditions and unexpected conditions related to user inputs (see Interactive Questions #11), testing for database integrity and performance (see Interactive Question #2), and testing of cybersecurity mitigations for unacceptable risks (see Interactive Question #10).

The table below shows the originally-provided testing documentation, and the additional testing documentation developed and performed during this review. Five test documents were supplemented with an additional 14 testing documents.

Original Submission	Test document description	Document reference
	(b) (4) Installation Qualification	IT-CSV-IMD14-06-IQ (Rev. 1.0)
	Operational/Performance Qualification	IT-CSV-IMD14-07-OPQ
	Supplemental (b) (4) Validation	IT-CSV-IMD14-07OPQb
	(b) (4) Operational/Performance Qualification	IT-CSV-IMD14-07-OPQ
	Executed (b) (4) Operational Performance Verification	IT- (b) (4) SPT-8 (Rev. 1.1)

Final documentation developed	Newly provided documentation	
	(b) (4) v1.0.5.5 Validation Plan	IT- (b) (4) SPT-10
	v1.0.5.5 Validation Report	IT- (b) (4) SPT-19
	Executed (b) (4) User Interface Verification	IT- (b) (4) SPT-14
	Executed (b) (4) PCR File Verification Test Protocol	IT- (b) (4) SPT-11
	Executed (b) (4) Unit Test Verification	IT- (b) (4) SPT-15
	(b) (4) Unit Test Report	IT- (b) (4) SPT-18
	Execute (b) (4) Installation Qualification	IT- (b) (4) SPT-9
	(b) (4) Database Server Migration Support Software Validation Plan	IT- (b) (4) SPT-22
	(b) (4) DB Availability Test Protocol	IT- (b) (4) SPT-17
	Cybersecurity test protocol	IT- (b) (4) SPT-24
	(b) (4) Software System Test Plan	IT- (b) (4) 1
	Software Verification Test Report	IT- (b) (4) 2
	Server Migration Plan	IT- (b) (4) SPT-29
	DB Migration Test Report	IT- (b) (4) SPT-31

10. Revision Level History: Acceptable

In the original submission, in the revision history (084_Attachment 4-5-10 Imugen (b) (4) revision level history.pdf) the applicant provided a revision level history which included updates that have been made through 8/28/2013.

Based on changes requested to correct an unresolved anomaly related to the NAT assay, the applicant provided an updated revision history (Attachment_14.1-IT-CSV-PDF-42&DocDetails.pdf) and updated design control documentation to support launch with version Build 1.0.5.5. See Interactive Question #12.

11. Unresolved Anomalies (Bugs or Defects): Acceptable

In the original submission, in the Unresolved Anomalies document (085_Attachment 4-5-11 Imugen (b) (4) Unresolved Anomalies_04172015.pdf) the applicant provided unresolved anomalies. Only one unresolved anomaly was reported, which is unrelated to the AFIA assay. This anomaly was ultimately corrected and resolved during the review of the NAT assay for BL 125588.

12. Cybersecurity: Acceptable

In the original submission, the applicant did not provide information on Cybersecurity. This includes, but is not limited to, the following facets of information security with respect to communications features of the device and associated software: confidentiality, integrity, availability and accountability.

- Confidentiality assures that no unauthorized users have access to the information.
- Integrity is the assurance that the information is correct - that is, it has not been improperly modified.
- Availability suggests that the information will be available when needed.
- Accountability is the application of identification and authentication to assure that the prescribed access process is being done by an authorized user.

Deficiencies were written for the Complete Response sent December 2015. See Appendix 1: Sponsor/Applicant Interactions and Communications, Interactive Questions #5, 6 and 10 for resolution of deficiencies related to cybersecurity.

Additional documentation was provided in the following, where the documentation was significantly updated.

- Complete Response received December 14, 2016
- Amendment received March 23, 2017
- Complete Response October 10, 2017
- Amendment received November 20, 2017

After the resolution of all deficiencies, the applicant provided a new risk management document specific to cybersecurity (046_Attachment-12.1_DOC-RSK-9_Cybersecurity Risk Assessment.xlsx) and additional testing for security-related risks (002_Attachment-1.1_IT-(b) (4)-SPT-24.pdf). A more detailed network diagram of the system was provided to assist in the identification of cybersecurity related risks, because the applicant has several computers and servers (b) (4). The IT business network is not completely isolated from the computers used to perform the assays. Interactions were required to help the applicant understand that simply adding a firewall was not an assurance that risks would be mitigated; instead, the applicant needed to specifically link identified security risks to the individual mitigations. Several references were provided to the applicant, including FDA's premarket and postmarket cybersecurity guidance documents. Finally, the applicant developed testing to ensure that the identified risk control measures were appropriate. Detailed interactions can be found in the Interactive Questions.

6 Reviewer Notes and Recommendations

a) Notes Related to the Review

- Significant interactive review occurred for both the NAT and AFIA submissions. Software and instrumentation questions for each overlap about 90%, although some questions were unique to each (e.g., PCR-specific questions for the NAT submission). While attempts were made to keep the numbering of the common questions the same, this was not possible.
- Due to an oversight, some common software and instrumentation questions were not included in the AFIA Information Request emailed February 24, 2017. The missing questions were however, included in the corresponding NAT IR sent February 17, 2017. Rather than send the questions separately, the issues were resolved in the NAT review memo, and the resolutions copied to Appendix 1: Sponsor/Applicant Interactions and Communications in response to the appropriate questions.
- Because this submission had an extra risk document related only to the AFIA assay, only this submission explored the new risk procedure, LAB-QA-62, that now applies to all risk activities at Oxford Immunotec. Summary information about the procedure is contained in the NAT memo, but detailed information is explored in this memo.

b) Notes of Disagreement

Specific software deficiencies were identified in September, 2015 but were not provided to the applicant until early 2017. This caused a significant delay of *over 16 months* in the applicant's ability to address the actual software and instrumentation deficiencies in their system. Specific deficiencies should be provided as early in the review cycle as possible.

c) Notes to Future Reviewers

Documentation changed significantly over the course of this review and many documents have been obsoleted. Refer to the October 10, 2017 (b) (4) Submissions Table" (036_Attachment-9.6_(b) (4) Submissions Table.pdf) from Amendment 27 for a list of all documents ever provided for this submission related to software and instrumentation. The table indicates when each was provided and if it is obsolete. **This table should be consulted before assuming any provided document is the latest version upon which this licensure is based.** Additionally, final risk documentation that applies to all risk procedures was provided in Amendment 33.

d) Reviewer Recommendation

When this submission was received, it was clear that the applicant did not have an adequate quality system in place when the design control documentation was developed. The quality of the documentation improved over the two Complete Responses and other information requests, especially after a consultant was retained to assist in development of adequate

processes. FDA participated in several interactive telecons and emails to provide supportive, guiding information on the applicant's evolving risk procedures. The biggest issues and improvements include:

- Risk processes and documentation improved significantly after the applicant developed a risk procedure aligned with ISO 14971 and harmonized the separate risk assessments for the NAT and AFIA assays.
- Verification and validation was initially limited to IQ and OPQ testing, which does not fully exercise the system. Additional testing was developed and completed to better align with unit, integration and system testing as outlined in FDA's premarket guidance document.
- No cybersecurity risk activities had been performed; a new cybersecurity risk assessment and cybersecurity testing have been implemented.

All deficiencies have been adequately resolved.

Reviewer Recommendation: Approvable. The following should be sent as described in Interactive Question #10 and reproduced below. No response is required.

In the amendment (001_Response to IR Received 9Nov2017_AFIA.pdf) received November 20, 2017 in response to FDA Question 3, you provided the versions of cybersecurity programs in use and stated that these are the latest version released and that you adhere to your policy of receiving automatic updates. Please note that at the time your response was prepared, both programs were currently advertised as having later versions of software than you provided. Therefore, you should ensure that your mechanism for receiving automatic updates is working correctly. No further response is required.

7 Appendix 1: Sponsor/Applicant Interactions and Communications

This appendix contains the resolution of all deficiencies in the form of Interactive Questions in “Question, Response, Comment” format.

The following questions were provided in a Complete Response letter dated September 29, 2015.

1. **FDA Question 34:** *In your BLA, you provided a Hazard Analysis (Attachment 4-5-4, (b) (4) Hazard Analysis.pdf) that includes potential hazards, severity estimation, hazard mitigation and updated severity estimation after hazard mitigation. However, information such as cause(s) of the hazard and verification that the method of control was implemented correctly are not included in your table. Your Hazard Analysis document should be in the form of an extract of the software-related items from a comprehensive risk management document, such as the Risk Management Summary described in ISO 14971. For example, Failure Mode and Effects Analysis (FMEA) can be one of the approaches that could be utilized to identify the hazards, their corresponding validation and verification and construction of the FMEA table accordingly. Therefore, please provide an updated table based on FMEA and ISO 14971 methodologies. For further information, please refer to the FDA software guidance document, <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089593.pdf>. Also, please consult a possible example of a FMEA table available at: <http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html>.*

Response: In the amendment received December 13, 2016 in response to FDA Question 34, the applicant provided risk analysis information including reference to the risk analysis, (b) (4) Risk Analysis IT-CSV-PDF-41.” The response was inadequate.

Comments: The following was supposed to be sent to the applicant on February 24, 2017 but was omitted from the SL’s memo. However, it was included in the February 17, 2017 communication for the NAT submission (BL 125588) as FDA Question 17. The resolution to this issue has been copied from the NAT memo and provided below, as it is applicable to this submission.

In your NAT Amendment response received December 14, 2016 in response to FDA Question 29 and in your AFIA Amendment received December 13, 2016 in response to FDA Question 34, you provided risk analysis information including reference to the risk analysis, (b) (4) Risk Analysis IT-CSV-PDF-41.”

- a. *In your response, you stated that the risk management document “[r]eferences mitigation plan, documented in SRS.” The file includes mitigations, but no numerical traceability from the risk ID to the SRS. Please provide this traceability. The Traceability Matrix “IT-CSV-IMD14-16-TM” embedded in your response document references Risk IDs that appear to be the Risk IDs in this document, but this is not*

explicitly stated. Please clarify this and provide updated documentation.

- b. This file does a better job of identifying individual risks than the document “B. microti AFIA Device Risk Analysis” (Attachment- 33.5_LAB-DSGN-5 .xlsx) and nicely allows the reader to use filtering to explore the effects of different causes and the scope of different mitigations. However, harm is not explicitly stated and too many “Potential Effects” are listed for each Risk ID. Some “Hazards” include cause information. Similar to the Device Risk Analysis, please update and provide this analysis to align better with ISO 14971 to leverage its benefits.*
- c. This file only references mitigations by “design.” Where have you documented the mitigations using other means; for example, in labeling that includes hazards or instructions? Please provide this information, including traceability from the individual mitigations to the corresponding user documentation where appropriate. This is necessary to review your proposed mitigations for risks that you have controlled through means other than by design.*

Note: this was resolved in the NAT submission, and the resolution cut-and-pasted below. All file references are to NAT documentation.

Response a: In the amendment received March 23, 2017 in response to FDA Question 17, the applicant provided an updated Traceability Matrix IT-CSV-IMD14-16-TM, “(b) (4) Traceability Matrix” (Attachment 15.2) with the requested traceability information. This is adequate.

Response b: In the amendment received March 23, 2017 in response to FDA Question 17, the applicant provided an updated FMEA risk analysis (Attachment_15.1-IT-CSV-PDF-41.xlsx) to better align with ISO 14971. The applicant refers to this as an “FMEA,” which it is not. It is table with some FMEA columns and some ISO 14971 columns but lacking sufficient information for either. There continues to be misunderstandings, as described in the Comments section below.

Response c: In the amendment received March 23, 2017 in response to FDA Question 17, the applicant stated that other mitigations requested are included in LAB-DSGN-11, “NAT Device Risk Analysis” and LAB-DSGN-5, “AFIA Device Risk Analysis”. The software specific risks are addressed in Attachment 15.1, IT-CSV-PDF-41, “(b) (4) Risk Analysis”. These updated documents were also referenced in the AFIA submission (BL125589) and the same concerns exist. Additional questions on content and harmonization are described in the Comments section below.

Comments: The following was sent to the applicant on April 14, 2017 as new FDA Question 9, and was included in the Complete Response letter sent June 13, 2017 as FDA Question 15:

Risk processes: In the NAT amendment received March 23, 2017 in response to FDA Question 17, you included updated risk documentation. There is some better alignment with ISO 14971 “Medical device – application of risk management to medical devices,” but the table in the (b) (4) Hazard Analysis (Attachment_15.1-IT-CSV-PDF-41.xlsx) is not an FMEA and does not align with terminology used in ISO 14971. Consider the following:

- a. What does your “Probability” correspond to in ISO 14971? It is not clear what your “Probability” refers to so it is difficult to assess the risk table. The “Scoring System” tab refers to Likelihood, not Probability. For example, Risk 2 “password hacked” has a Probability of 4 which is high, so it is unclear if this refers to P1 or P2 or the combination. In the “Front page” tab of the NAT Risk Analysis (Attachment_22.1-LAB-DSGN-11.xlsm), the Likelihood definitions specifically refer to failures. This suggests that your probability is still focused only on P1 and does not include probability of a hazardous situation leading to harm. Please revisit your risk management processes and provide a clear description of your processes and how they align with ISO 14971. State explicit the scope of “probability” in your documentation and ensure your risk documentation includes all aspects of probability. As a start, we suggest removing the notion of “failure” from your definitions.*
- b. What is your process to determine the new level of Probability as the result of the identified mitigation(s)? Please provide your risk documentation that describes how this is determined.*
- c. Please refer to comments made regarding the “Babesia microti AFIA device risk analysis” (Attachment_13.1-LAB-DSGN-5.xlsm) and its alignment with ISO 14971, and ensure that you make the same changes to both risk documents for consistency regarding clear traceability with hazards, hazardous situations, causes, traceability to mitigations in manuals and SOPs, etc. We recommend that you should harmonize the format you are using to capture risk information so that all use the same terminology and methods, or you should provide a clear description and process for each that allows independent review.*

Response: In the complete response (001_BL125588-NAT Complete Response.pdf) received October 10, 2017 in the response to FDA Question 11 on PDF page 25, the applicant provided updated risk management information.

(a) The applicant stated that they revised their risk assessment processes to comply with ISO 14971 in LAB-MEM-38, “Memo on Risk Management” (Attachment 6.9). Several changes in their processes were made, such as ensuring potential causes related to a specific hazard and foreseeable events are documented with specific links to outcome malfunctions. Hazardous situations are clarified and assessed according to ISO 14971, probability of harm from hazardous situations has been added, a “risk probability number” is added, and mitigations are assessed individually to determine effects on risks separately. Risks to harm from both manufacturing process failure and assay process failure are included. The risk

processes are significantly improved from previous submissions. A note about a conflict with the term, “Risk Probability Number” should be sent to clarify any confusion – see the Comments section.

(b) Methods to determine the new probability level are included in the memo, with examples in Section 3. This is adequate.

(c) The applicant stated that the risk formats were harmonized as requested. This is adequate.

Comments: The following was emailed to the applicant on November 9, 2017 as new FDA Question 4.

In the complete response, in your Memo on Risk Management (029_Attachment-6.9_LAB-MEM-38& Doc Details.pdf) you described updates to your risk assessment methods to comply with ISO 14971 and provided clear instructions and examples. As a minor note, you defined “Risk Probability Number (RPN)” as the product of Severity, P1 and P2. Calculating risk this way is acceptable. However, please be aware that the acronym “RPN” is used heavily in industry as “Risk Priority Number” and refers to a different concept. To avoid confusion, you should refer to your risk calculation differently (perhaps “Risk Number (RN)”), or simply call it what it is: Risk.

Response: In the amendment (001_Response to IR Received 9Nov2017_NAT.pdf) received November 20, 2017 in response to FDA Question 4, the applicant stated that the terminology has been modified and documents will refer to “Risk Number” and “RN”.

Comments: The response is acceptable. Resolved.

2. **FDA Question 35:** *You provided Software Requirements Specifications (SRS) in the document (b) (4) Software Requirements Specification” (Attachment 4-5-5 SRS(b) (4) IMUGEN.pdf) that describes the client/servicer application. The document includes 20 requirements for hardware, interface, software, performance, regulatory, system backup and restore. Most requirements are too high level and do not include testable information. The requirements for workflow processes, boundary conditions and error recovery are missing. Please provide a modified version of the Software Requirements Specification document, which should clearly document the functional, performance, interface, design and development requirements.*

Response: In the amendment received December 13, 2016 in response to FDA Question 35, the applicant provided an updated SRS where information has been inexplicably removed. The response was inadequate.

Comments: The following was supposed to be sent to the applicant on February 24, 2017 but was omitted from the SL’s memo. However, it was included in the February 17, 2017 communication for the NAT submission (BL 125588) as FDA Question 16. The resolution

to this issue has been copied from the NAT memo and provided below, as it is applicable to this submission.

In your original submission in the software requirements document (Attachment 4-5-5 SRS-(b) (4) IMUGEN) in Section 2.5 you provided Performance Requirements. In your NAT Amendment response received December 14, 2016 in response to FDA Question 30 and in your AFIA Amendment response received December 13, 2016 in response to FDA Question 35 you provided an updated Software Requirements Specification document where all performance requirements were removed. Please clarify why entire sections of requirements have been removed, and update and provide your requirements documentation to ensure all requirements are correctly captured.

Note: this was resolved in the NAT submission, and the resolution cut-and-pasted below. All file references are to NAT documentation.

Response: In the amendment received March 23, 2017 in response to FDA Question 16, the applicant stated that requirements “relevant to IT infrastructure for general lab operation ... is beyond the scope of the (b) (4) software” and were removed. Unfortunately, performance requirements are very relevant for their throughput and capacity claims, which don’t appear in the requirements. These should be added back, with testable criteria, and corresponding test results to show that the underlying infrastructure can support the device intended use.

Comments: The following was sent to the applicant on April 14, 2017 as new FDA Question 1, and was included in the Complete Response letter sent June 13, 2017 as FDA Question 6:

Performance requirements for (b) (4) hardware and software: In the NAT amendment received March 23, 2017 in response to FDA Question 16, you stated that requirements “relevant to IT infrastructure for general lab operation ... is beyond the scope of the (b) (4) software and were removed.” This is not reasonable because the (b) (4) software requires proper operation of the underlying infrastructure to meet its intended use. Your documentation has inconsistently described the components of the system, and it is not clear what hardware supports the (b) (4) software and database functionality. You should include requirements related to the infrastructure that is necessary to support the intended use of the device for both the NAT and AFIA assays. This appears to include the components in the Hardware Network Diagram in section 2.3.2 in your Architectural Design document provided in Attachment 29.4 of your response received December 14, 2016, and any other relevant components not identified in this diagram.

- a. Please clarify all of the required components for your system, including PCs, printers, network connections, etc. Explicitly identify the boundaries of the system with respect to your corporate network.*
- b. Please include all requirements related to required capacity for throughput, database capacity and accessibility, connectivity, uptime, etc., in order for the underlying*

infrastructure system to meet the required needs of the system. These requirements should include testable metrics to ensure that they can be met.

- c. Include all test plans, test results and verification and validation testing for these performance requirements.*
- d. Update your traceability matrix to include this information.*
- e. Update your risk documentation to include risks associated with the performance needs of the system, and include the mitigations you implemented to reduce those risks to acceptable levels.*

Response: In the complete response (001_BL125588-NAT Complete Response.pdf) received October 10, 2017 in the response to FDA Question 6 on PDF page 7, the applicant provided additional information.

- (a) Architectural design information and updated components of the system were provided to illustrate system boundaries and facilitate development of the applicant's risk documentation.
- (b) Requirements were updated and untestable requirements were changed to address the issues. Untestable specifications were corrected and retested. Additional requirements were added to ensure the infrastructure can support (b) (4) performance needs.
- (c) An FDA consultant was hired who reviewed testing of performance requirements; updated test plans and results were provided.
- (d) Updated traceability was provided.
- (e) Risk documentation was updated with performance-related risks and countermeasures implemented to reduce risk to acceptable levels.

Comments: The response is acceptable. Resolved.

- 3. **FDA Question 36:** *You did not provide an Architectural Diagram that shows a description of the software system partitioned into its functional subsystems, including a description of the role that each module plays in fulfilling the software requirements. Please provide an Architectural Diagram of your software. It is recommended that you consult ISO 62304 (Medical device software -- Software life cycle processes) to prepare your software documentation and conduct testing.*

Response: In the amendment received December 13, 2016 in response to FDA Question 36, the applicant provided an updated architecture diagram in Attachment 34.4.

Comments: This response is acceptable. Resolved.

- 4. **FDA Question 37:** *You provided a software design specification document (Attachment 4-5-6 SDS (b) (4) IMUGEN.pdf) for the (b) (4). The document includes the modules of the (b) (4) for Process Role, IFA Role, Report Role, Audit*

Role, and Admin Role. These each illustrate the control flow among the User, the UI, the Data Model and the Data Storage. The database schematic is presented in Figure 1 on page 886-888, definitions are included in Section 2.4 starting on page 889 and all components are described by Field with included Notes and Type. However, none of the fields have specified measureable or testable values. There is no traceability from the requirements enumerated in document "Attachment 4-5-5 SRS-(b) (4)IMUGEN.pdf" to this SDS document to describe how the requirements in the Software Requirements Specifications (SRS) are implemented. Please add the missing requirements to your software requirements specifications, including all step-by-step workflow requirements, for both AFIA and NAT, and provide all updated design control documentation that is affected.

Response: In the amendment received December 13, 2016 in response to FDA Question 37, the applicant provided an updated SDS in Attachment 34.5 that is missing testable details and test case information. The response was inadequate.

Comments: The following was supposed to be sent to the applicant on February 24, 2017 but was omitted from the SL's memo. However, it was included in the February 17, 2017 communication for the NAT submission (BL 125588) as FDA Question 18. The resolution to this issue has been copied from the NAT memo and provided below, as it is applicable to this submission.

In your NAT Amendment response received December 14, 2016 in response to FDA Question 32 and in your AFIA Amendment received December 13, 2016 in response to FDA Question 37, you stated that for the (b) (4) software, you included an updated Software Design Specification and Traceability Matrix that "contain measurable and testable values." Thank you for providing these updates and the detailed information. Several Risk ID/SRS entries in your traceability table do not trace to software design specifications, and some trace to testing that does not appear to relate to the corresponding risk/requirement. This makes it difficult to assess the adequacy of your proposed mitigations. Note that necessary testing at the unit, integration and system level is often different and more comprehensive than qualification testing.

- a. *For example, Risk ID 24/SRS 24 addresses a risk that PCR results might be modified. No design information was provided on how this would be performed, and the referenced V&V test cases don't appear to test any attempts to modify PCR results to ensure the risk is properly mitigated. The tests are "Script (b) (4) and "Script (b) (4) Step # (b) (4) How do these tests verify that software prevents any modification of the PCR results? Please provide the correct documentation.*
- b. *Risk ID 34/SRS34 involves risk of loss of sample origin, but has no associated SDS. The requirement itself is vague and the corresponding testing refers to step # (b) (4) of a test script. However, the test script ends after (b) (4) steps. Please clarify the risk and*

requirement, and provide corrected documentation.

- c. Risk ID 39/SRS 39 refers to a test script that was not provided. This portion of the testing documentation is blank. Please provide the correct documentation.*
- d. Risk ID 49/SRS 49 does not include testable information and is not traceable to an SDS. Some of the relevant information appears in the test case; however, specifics of the device design should be captured in the requirements and specification documentation, and not documented solely in testing documentation. Please update your SRS and/or SDS with the appropriate design information accordingly, and provide the correct documentation.*
- e. Risk ID 51/SRS 51 and Risk ID 52/SRS 52 specify software by version number “or later.” Your requirements should apply to a specific version or versions with testing corresponding to those versions. Please remove reference to “or later” for any software used in the system, including in any labeling, and ensure explicit versions are referenced.*

This is not a complete list of issues, but a representative sample of concerns. Please review and update the remainder of the document for traceability and accuracy issues. For requirements that have no corresponding design specification, clarify why an SDS is not necessary.

Note: this was resolved in the NAT submission, and the resolution cut-and-pasted below. All file references are to NAT documentation.

Response: In the Amendment received March 23, 2017 in response to FDA Question 18, the applicant addressed each of the Risk/SRS pairs enumerated in the FDA Question: (a) was clarified, (b) has been corrected with correct validation, (c) supplemental testing was provided. For (d), testing details were augmented, (e) references to “or later” were removed, and traceability and SRS documents were updated accordingly.

Comments: The response is acceptable. Resolved.

Response 2: In the amendment received December 13, 2016 in response to FDA Question 37, the applicant provided an updated SDS in Attachment 34.5 that does not contain explicit design specification information traceable to requirements. The response was inadequate.

Comments 2: The following was supposed to be sent to the applicant on February 24, 2017 but was omitted from the SL's memo. However, it was included in the February 17, 2017 communication for the NAT submission (BL 125588). The resolution to this issue has been copied from the NAT memo and provided below, as it is applicable to this submission.

In your NAT Amendment response document received December 14, 2016 in response to FDA Question 32 and in your AFIA Amendment response received December 13, 2016 in response to FDA Question 37, you provided a Software Design Specification document. This version 1.1 of the document does not appear to be substantially changed over version 1.0 provided in your original submission. Many screen shots are presented but it is not always apparent what has changed from one screen to the next, what is expected to appear on the screen, what information the user entered, and what are the system responses when the user does something unexpected. Each of these specifications should include explicit text about what should appear on the screen and what the device and/or user is expected to do. It is not sufficient to collect screen shots of a completed system and state that these encompass a software design specification without additional information. It is not reasonable to expect a designer/tester/reader to compare successive screen shots to determine for themselves what has changed between the two screen shots. This increases the opportunity for misunderstanding, inadequate design and testing.

Please augment the information in your Software Design Specification with explicit testable information. Some of this information appears to exist in various testing documents and SOPs, but you have not provided a comprehensive collection of software design specifications which describes how the requirements in the Software Requirements Specifications (SRS) are implemented in a clear and unambiguous manner. Please provide this updated information.

Note: this was resolved in the NAT submission, and the resolution cut-and-pasted below. All file references are to NAT documentation.

Response: In the Amendment received March 23, 2017 in response to FDA Question 19, the applicant provided updated versions of the Risk Analysis, Traceability Matrix, SRS and SDS referred to above (Attachments 15.1, 15.2, 15.3 and 18.1, respectively). The Software Design Specification contains significantly more detailed and testable information to accompany the previous screen shots, and the corresponding testing is provided and included in the other design documentation.

Comments: The response is acceptable. Resolved.

5. **FDA Question 38:** *You provided a traceability document (Attachment 4-5-7 IMUGEN (b) (4) Traceability Analysis.pdf) that includes items for each of 22 high level requirements.*

The “Verification and Validation Tests” in the form of references to Installation Qualification tests or Operational/Performance Qualification tests are included and the associated hazards are identified. The traceability of requirements and specifications to testing and hazards are not comprehensive. This is due in part to inadequately formulated requirements which are often vague and untestable as written, and the use of test cases which are mostly limited to using valid values and workflow actions.

- a. Please provide verification and validation information for all software requirements (including missing requirements mentioned in other deficiencies), which should include the unit, integration and system level test protocols, including the pass/fail criteria, and test report, summary and test results.*
- b. Please provide traceability information described at the detail level of individual software requirements rather than the high level software requirements, R1-R22. This includes traceability among identified clinical hazards and mitigations, requirements, specifications, and verification and validation testing in an enumerated manner.*

Response: In the amendment received December 13, 2016 in response to FDA Question 38, the applicant provided an updated traceability matrix in Attachment 34.3. The applicant enumerated each of 58 Risk IDs and corresponding requirements, and stated that testing information appears in relevant IQ and OPQ reports. IQ and OPQ testing are not the same as verification and validation testing outlined in part (a); the applicant did not provide adequate testing documentation. The response was inadequate.

Comments: The following question was included in the AFIA Complete Response letter sent June 13, 2017 as FDA Question 9. The applicant was informed that some AFIA questions contained NAT references, but applied to both.

In the NAT amendment received December 14, 2016, in response to FDA Question 33, you provided an updated traceability matrix in Attachment 29.3 and referred to IQ and OPQ testing. The testing is incomplete. Note that process validation testing (Installation Qualification (IQ), Operational Qualification (OQ) and Performance Qualification (PQ)) testing are not the same as verification and validation testing outlined in part (a) of Question 33. Please refer to FDA’s guidance document, “General Principles of Software Validation,” with a particular focus on section 5.2.5, located at <https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085371.pdf>. As outlined in the premarket software guidance, “Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices,” please ensure that you provide unit, integration and system level test protocols, including pass/fail criteria, test report summary, and tests results. It is difficult to assess the adequacy of a test script by viewing only raw test steps without a description of the test plan and protocol and a summary of results.

Response: Identical information was provided for the NAT and AFIA responses, although an additional follow-up question was sent for the NAT that also applies here. Therefore, what appears below is the NAT resolution of this common deficiency:

In the NAT complete response (001_BL125588-NAT Complete Response.pdf) received October 10, 2017 in the response to FDA Question 7 on PDF page 12, the applicant provided Attachment 13.3, “(b) (4) Submissions Table” that indicates all documents sent to the FDA with their date of submission, the relevant attachment number, the relevant software version, and whether the document is now obsolete. This is extremely helpful because multiple versions of documents have been sent over the last two years. Table 7.1 on page 14 lists all the individual types of tests performed, an explanation of the test, justification, and test activity (with file name).

The testing plan and strategy for v1.0.5.5 was provided, and was revised to include unit, integration, and system level testing. The updated test plan and test report were provided for version Build 1.0.5.5 (024 Attachment-6.4_IT(b) (4)-1 &Doc Details.pdf, 025_Attachment-6.5_IT(b) (4)-2 &Doc Details.pdf) and includes the testing types and computers involved. All requirements were met.

Comments: The following was emailed to the applicant on November 9, 2017 as new FDA Question 1.

In the complete response (001_BL125588-NAT Complete Response.pdf) received October 10, 2017 in the response to FDA Question 7 on PDF page 12, you provided a table of testing activities. We were unable to locate the test protocol results that correspond to IT(b) (4) - SPT-24 “(b) (4) CyberSecurity Test Protocol” and IT(b) (4)-SPT-17 (b) (4) System Uptime Test Protocol.” Please provide these test case results. This is necessary to confirm the claim that all requirements have been correctly implemented.

Response: In the amendment (001_Response to IR Received 9Nov2017_NAT.pdf) received November 20, 2017 in response to FDA Question 1, the applicant stated that the test results were inadvertently omitted, and provided the requested information. The testing is adequate.

Comments: The response is acceptable. Resolved.

6. **FDA Question 39:** *You did not provide information on Cybersecurity related to all instruments, hardware and software incorporated into the system, including Off-the-Shelf components. The (b) (4) system includes at least (b) (4) types of servers and multiple workstations/clients, at least (b) (4) of which has established connectivity to the outside world. Please provide information on the Cybersecurity aspects of your device, including, but not limited to, the following facets of information security with respect to communication features of your device, associated software and other required components: confidentiality, integrity, availability and accountability. Confidentiality assures that no unauthorized users have access to the information. Integrity is the assurance that the information is correct -*

that is, it has not been improperly modified. Availability suggests that the information will be available when needed. Accountability is the application of identification and authentication to assure that the prescribed access process is being done by an authorized user.

Response: In the amendment received December 13, 2016 in response to FDA Question 39, the applicant provided an Information Technology Security Policy in Attachment 34.6 that is not related to security concerns during device operation. The response was inadequate.

Comments: The following was supposed to be sent to the applicant on February 24, 2017 but was omitted from the SL's memo. However, it was included in the February 17, 2017 communication for the NAT submission (BL 125588) as FDA Question 20. The resolution to this issue has been copied from the NAT memo and provided below, as it is applicable to this submission.

In your NAT Amendment response received December 14, 2016 in response to FDA Question 35 and in your AFIA Amendment received December 13, 2016 in response to FDA Question 39 with respect to cybersecurity, you provided the document, "Information Technology Security Policy, IT-SEC-POL-1." You stated that this describes "control of confidentiality information and accountabilities." This policy appears to apply to your corporate networks and business policies rather than for the device itself. Please note that you should identify risks associated with not only confidentiality, but integrity and availability, and take steps to reduce risk that device functionality is intentionally or unintentionally compromised by inadequate cybersecurity considerations. The (b) (4) system appears to include at least (b) (4) types of servers and multiple workstations/clients, at least (b) (4) of which has established connectivity to the outside world. Your risk documentation appears to contain some mitigations for potential cybersecurity risks, although you have not identified many of the possible causes to demonstrate that these mitigations would be adequate.

- a. Please refer to the FDA guidance and provide updated cybersecurity information for your device to address the elements listed in the guidance: "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" located at <http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidanc edocuments/ucm356190.pdf>. This should include, in part, the following: hazard analysis, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with your device, and a traceability matrix that links your actual cybersecurity controls to the cybersecurity risks that were considered.*
- b. Please describe your process for identifying and evaluating new operating system patches and other updates to off-the-shelf software and integrating patches and updates into your device.*

Note: this was resolved in the NAT submission, and the resolution cut-and-pasted below. All file references are to NAT documentation.

Response: In the Amendment received March 23, 2017 in response to FDA Question 20, the applicant stated the referenced information was reviewed. In response, the applicant created a “Business Continuity and Disaster Recovery Plan” (Attachment 20.1 Attachment_20.1-DOC-POL-1.pdf) that focuses on business risk and includes data backup and recovery plans. The applicant also provided a substantial update to the “Information Technology Security Policy” (Attachment_20.2-IT-SEC-POL-01&DocDetails.pdf) that includes policies for accounts management, password management, encryption, data security, and software patches and updated, including antivirus updates. The applicant also pointed to the updated “(b) (4) Risk Analysis” (Attachment_15.1-IT-CSV-PDF-41.xlsx). These are not adequate to answer the questions posed.

The applicant has not provided documentation aligned with the FDA guidance document. The risk management should include entries for all identified cybersecurity related risks to link these risks to the mitigations implemented, but this has not been done.

Comments: The following was sent to the applicant on April 14, 2017 as new FDA Question 10, and was included in the Complete Response letter sent June 13, 2017 as FDA Question 16:

Cybersecurity considerations: In the NAT Amendment received March 23, 2017 in response to FDA Question 20, you provided several documents including an updated “(b) (4) Risk Analysis” (Attachment_15.1-IT-CSV-PDF-41.xlsx). Please note that we assess the adequacy of your cybersecurity features based on the threats and vulnerabilities you identify in your risk assessment. Without your analysis and identification, it is difficult for us to determine if the mitigations you implement are adequate. We do not have a clear picture of the client server and database components and connectivity to other systems. We see mention of some mitigations and some evidence of threats in several documents, but you have not provided a comprehensive view of the security risks to your system. The following suggest that the analysis activities we requested and described in the cybersecurity premarket guidance have not occurred.

- Your system is networked but you have no requirements or specifications related to connectivity or use of a firewall. You included a firewall in the Hardware Network Diagram in your Architectural Design document in Attachment 29.4 of your response received December 14, 2016, but it is not referenced in your risk documentation. You have not identified which risks might be addressed by use of a firewall, and the residual risks. You have not identified vulnerabilities related to this architecture.*
- You reference antivirus updates in your “Information Technology Security Policy” (Attachment_20.2-IT-SEC-POL-01&DocDetails.pdf) but you have not identified the vulnerabilities for which this mitigation would be effective. It also mentions physical*

security, but it is not clear if or how this applies to access to the software or hardware.

- *Some features that represent suggest security vulnerabilities were not included; for example you mention USBs in the “Information Technology Security Policy” but you have not discussed the risks of allowing an open USB port.*
- *You have not identified functionality on the computer that should be restricted to limit exposure (e.g., disabling access to various unnecessary programs, unauthorized access through unattended workstation availability, etc.). Can users access the internet on the computer used to access the (b) (4) software? Can a user boot from a USB and alter the system? Can a user replace the (b) (4) software with an altered copy? Many scenarios related to misuse have not been explored.*

As requested previously, please perform the analysis described in the guidance, “Content for Premarket Submissions for Management of Cybersecurity in Medical Devices” and updated your design documentation accordingly.

Response: In the complete response (001_BL125588-NAT Complete Response.pdf) received October 10, 2017 in the response to FDA Question 12 on PDF page 27, the applicant provided requested information and stated that their design documentation was updated to align with the analysis described in the premarket cybersecurity guidance document, as outlined on page 32.

- (a) The applicant stated that a full review of security risks was conducted using the new risk management procedure (Attachment 6.9) and documented in the cybersecurity risk analysis DOC-RSK-9, “Cybersecurity Risk Analysis” (Attachment 12.1). Traceability to associated design control documentation was provided. The response document provides a good overview of the analysis.
- (b) The applicant clarified the vulnerabilities and relevance of the document in Tables 12.4 and 12.5 on page 30.
- (c) The applicant stated risks of unsecured USBs and other external device ports is included in the Cybersecurity Risk document, DOC-RSK-9 (Attachment 12.1) and enumerated in Table 12.6 on page 31.
- (d) The applicant provided the Cybersecurity Risk Assessment (DOC-RSK-9, Attachment 12.1) that includes risks and appropriate mitigations for potential computer misuse. (b) (4) vulnerabilities were identified and discussed in Table 12.7 on page 32.

Comments: The response is acceptable. Resolved.

7. **FDA Question 40:** *You stated that “laboratory managers will use the software to produce reports of sample results which are electronically transmitted to the submitting entity” (page 867, Attachment 4-5-5 SRS-(b) (4)_IMUGEN-20150324). However, it is not clearly described how these results are transmitted to these facilities. As your service expands in the*

future, you will be collecting and reporting greater amounts of data. Please explain how these data will be managed and coordinated between your laboratories and blood establishment facilities.

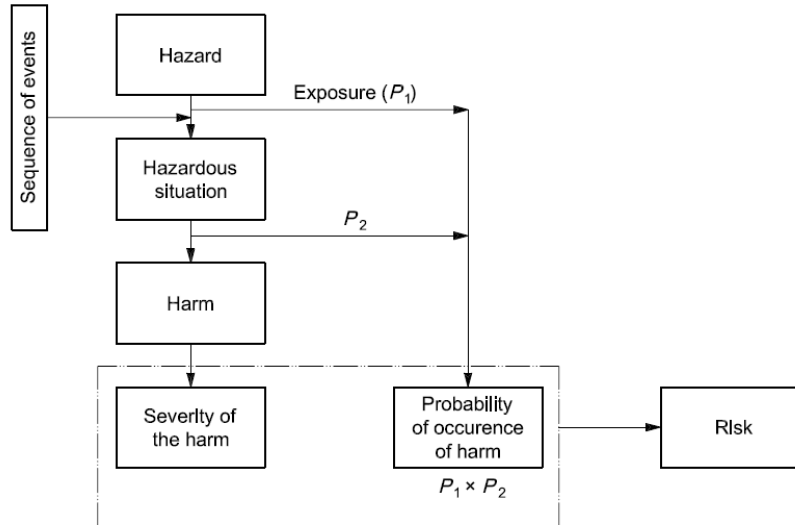
Response: In the amendment received December 13, 2016 in response to FDA Question 40, the applicant stated that reports are sent manually by email in PDF format or as .csv file via secure FTP. The response is acceptable.

Comments: The response is acceptable. Resolved.

The following questions relate only to the Babesia AFIA (amendment received December 13, 2016) submission and were sent to the applicant on February 24, 2017:

8. **FDA Question 13:** *In your AFIA Amendment response received December 13, 2016 in response to FDA Question 34 you stated that you used FMEA and ISO 14971 methodologies for your Risk Analysis, and you provided the document “B. microti AFIA Risk Analysis” (Attachment- 33.5_LAB-DSGN-5 .xlsx). In the tab “Front page” you provided a risk matrix and described levels for “Severity” and “Likelihood” to estimate risk. Your definition of likelihood values focuses on failures and the frequency that a failure would occur; however, this does not align with likelihood or probability in ISO 14971, which focuses on occurrence of harm rather than failure. Risk in ISO 14971 is the combination of the probability of occurrence of harm and the severity of that harm. Risk estimation considers two likelihoods: the likelihood of a hazardous situation occurring and the likelihood of the hazardous situation leading to harm. These are both considered when determining the overall probability of harm for a particular combination of events. Figure E.1 from ISO 14971 provides a good pictorial representation of the relationship of hazard, sequence of events, hazardous situation, and harm.*

It is not clear how your use of “likelihood” captures the probability portion of risk as outlined in ISO 14971. Please provide your processes related to risk management and explain how your processes align with ISO 14971. We recommend that you revisit how you define “likelihood” so that it is better aligned with ISO 14971 and provide an update on your risk analysis table. This should be aligned with the risk-related requests elsewhere in this communication.



NOTE P_1 is the probability of a hazardous situation occurring.
 P_2 is the probability of a hazardous situation leading to harm.

Response: In the Amendment received March 20, 2017 (AFIA Information Request Response.pdf), in response to FDA Question 13, the applicant stated that the risk analysis was updated to better align with ISO 14971, and provided an update risk analysis table “Babesia microti AFIA device risk analysis” (Attachment_13.1-LAB-DSGN-5.xlsm) and report of the reanalysis: “Re-Analysis of Risk Assessment LAB-DSN-5” (Attachment_13.3-DOC-RPT-91.pdf). The applicant did not provide a description of how “likelihood” is used, but blindly changed all instances of “likelihood” to “probability” without acknowledging these are not interchangeable.

Comments: The response is inadequate. Additional information is required as described below. The following two new questions related to the risk management process were sent to the applicant in the AFIA Complete Response letter dated June 13, 2017. The first was sent as new FDA Question 12 (below), the second as FDA Question 13 (directly after):

FDA Question 12: Risk Management and ISO 14971 alignment: *In the Amendment received March 20, 2017 in response to FDA Question 13, you provided updated risk information. We requested that you describe how your processes align with ISO 14971 but you did not provide an explanation. Language in your “Re-Analysis of Risk Assessment LAB-DSN-5” (Attachment_13.3-DOC-RPT-91.pdf) suggests misunderstandings in the application of ISO 14971 “Medical device – application of risk management to medical devices.” We are attempting to understand what you changed by comparing your previous risk documentation to the latest documentation in order to identify what should be addressed.*

- a. *In your document “Re-Analysis of Risk Assessment LAB-DSN-5” (Attachment_13.3-DOC-RPT-91.pdf) in Table 3 in response to FDA Question 13, you provided estimates of Probability of Harm. Table 1 includes Failure Effect Codes mapped to*

both severity and probability. Specifying Severity for a particular harm is appropriate. However, please note that estimates of probability of harm are made within the context of each identified hazard and hazardous situation, and assigning probability of harm to a failure effect as you have done (independently of the hazardous situations and causes) is not consistent with risk analysis as outlined in ISO 14971. You can't explicitly state the probability without a discussion of the hazardous situation that could allow that particular harm to occur. It is not logical to assume that every situation that could result in a false negative (for example) is associated with a high probability of harm. The different potential causes and resulting hazardous situations will affect the value of probability for that particular situation. Table 1 should be changed to align with ISO 14971, and the direct mapping to "Probability of Harm" removed.

- b. In concert with part (a) above, the "Probability of Harm" in the document "Babesia microti AFIA device risk analysis" (Attachment_13.1-LAB-DSGN-5.xlsm) should be updated to reflect your assessment of "Probability of occurrence of harm" as a combination of probability of the hazardous situation occurring and the probability that the hazardous situation leads to harm. You do not need to identify P1 and P2 in this document, but your assessment of "Probability" should be specific to the "Potential Cause(s)" that you have identified. This is one reason why you have listed each cause as a separate row in the risk table, because each might be associated with a different value of Probability.*
- c. You have added the term "failure effect" to your risk documentation. This term is used in FMEAs but is not used in ISO 14971. Please clarify how this maps to your support of ISO 14971. Your document "Re-Analysis of Risk Assessment LAB-DSN-5" (Attachment_13.3-DOC-RPT-91.pdf) does not explain how failure effects are related to harms, because they are not the same thing. One failure effect may be associated with more than one kind of harm; for example, a false positive and a false negative are generally associated with different harms and have different severities and sometimes different probabilities of harm. However, you combined false negative and false positive in several cases. You should consider consistently adopting terms from ISO 14971 and be consistent with a particular methodology. Please update your risk documentation accordingly. We suggest removing "failure effect" and including columns consistent with ISO 14971.*
- d. In the document "Babesia microti AFIA device risk analysis" (Attachment_13.1-LAB-DSGN-5.xlsm) it appears you eliminated the term "likelihood" and replaced it with "probability." In the "Front page" tab, the Probability definitions specifically refer to failures. This suggests that your probability is still focused only on P1 and does not include probability of a hazardous situation leading to harm. Please revisit your risk management processes and provide a clear description of your processes and how they align with ISO 14971. State explicit the scope of "probability" in your documentation and ensure your risk documentation includes all aspects of*

probability. As a start, we suggest removing the notion of “failure” from your definitions. Note that this will require more than changing column names and definitions, but will require that you ensure each row in the table is specific to one cause/situation, and that the value of Probability is the probability that the cause/situation would lead to harm. Harm should be added to the table. This is necessary to produce an assessment that is aligned with ISO 14971.

Response: In the amendment received October 10, 2017 (001_BL125589 AFIA Imugen Complete Response.pdf) in response to FDA Question 13 on page 24, the applicant stated that the risk management approach has been changed to be consistent with ISO 14971 and included a “Memo on Risk Management” (Attachment 12.1) that describes the new approach.

Several changes in the processes were made, such as ensuring potential causes related to a specific hazard and foreseeable events are documented with specific links to outcome malfunctions. Hazardous situations are clarified and assessed according to ISO 14971, probability of harm from hazardous situations has been added, a “risk probability number” is added, and mitigations are assessed individually to determine effects on risks separately. Risks to harm from both manufacturing process failure and assay process failure are included. The risk processes are significantly improved from previous submissions. A note about a conflict with the term, “Risk Probability Number” should be sent to clarify any confusion – see the Comments section. Methods to determine the new probability level are included in the memo, with examples in Section 3. A follow-up question was sent in the NAT submission to suggest “RPN – Risk Probability Number” be changed to “RN” or “Risk Number” to avoid confusion with the common industry term, Risk Priority Number. The applicant agreed to make the change. See the very end of Interactive Question 1 in the NAT memo.

Comments: The response is acceptable. Resolved.

FDA Question 13: *Risk management process: In the Amendment received March 20, 2017 in response to FDA Question 13, you stated that you updated your risk analysis to better align with ISO 14971. You should have procedures that describe your risk management process. Your process appears to have changed as a result of your last amendment with the elimination of “likelihood” from your risk analysis and other changes as described in your document “Re-Analysis of Risk Assessment LAB-DSN-5” (Attachment_13.3-DOC-RPT-91.pdf). We are trying to locate the relevant processes/procedure(s) because they don’t appear to be aligned with ISO 14971.*

In section 2 of the re-analysis document, you stated that the risk analysis was performed according to “LAB-QA-62 Risk Management Procedure.” However, in response to FDA Question 33 in your response document (001_AFIA Response to AI p 1 to 260.pdf) received December 13, 2016, you stated on page 35 that LAB-QA-62 was obsoleted and that the information was included in the revised LAB-QA-67 (Attachment 33.3). We reviewed the

Design and Development Procedure (LAB-QA-67) (003_AFIA Response to AI p 497 to 737.pdf); however, LAB-QA-62 is not listed as obsolete, but is referenced for use in developing the Risk Analysis.

Please provide the document LAB-QA-62 and any other risk related procedures that apply to the NAT and AFIA assays and to the (b) (4) software and associated hardware. Because it appears that you have updated your processes, please provide the latest documentation describing how you perform your risk related procedures.

Response: In the amendment received October 10, 2017 (001_BLI25589 AFIA Imugen Complete Response.pdf) in response to FDA Question 12 on page 21, the applicant stated the risk process was revised to be consistent with ISO 14971 and referred to the provided “Memo on Risk Management (Attachment 12.1) that describes the changes. The applicant stated, “we wish to clarify that the original LAB-QA-62 (“Risk Management”) was obsolete and replaced with a revised, global document, “Product and Process Risk Management.” However, that document was not provided.

Comments: The following was sent to the applicant on November 11, 2017 as new FDA Question 5.

In the complete response (001_BLI25589 AFIA Imugen Complete Response.pdf) received October 10, 2017 in the response to FDA Question 12 on PDF page 22, you stated that revisions are occurring on the obsolete LAB-QA-62 risk management procedure, and that it will become the company-wide “Product and Process Risk Management” document. Please provide the updated document and clarify its relationship to the provided LAB-MEM-38 “Memo on Risk Management.” This is necessary to review your updated and finalized risk management procedure.

Response: In the amendment received November 20, 2017 (001_Response to IR Received 9Nov2017_AFIA.pdf) in response to FDA Question 5 on page 4, the applicant introduced the “now activated company-wide procedure for risk management LAB-QA-62 ‘Product and Process Risk Management’ (Attachment 5.1).” The applicant’s explanation is provided below:

“The company-wide “Procedure for Risk Management” encompasses each product and service manufactured and operated by Oxford Immunotec Ltd., Oxford Immunotec Inc., Oxford Diagnostic Laboratories and Imugen. The scope of the procedure covers products with varied intended uses and users, therefore provides an overall instruction for the application of risk management.

“LAB-MEM-38 provides a logic flow from the application of LAB-QA-62, the updated company-wide Risk Management procedure (Attachment 5.1), to both the B. microti AFIA and NAT tests, and was intended to provide the guidelines for the overall instruction of risk

management laid out in LAB-QA-62, “Product and Process Risk Management”, prior to its companywide activation.”

The content of the document is discussed in the Device Hazard Analysis in Section 5, Software and Instrumentation Documentation Status and Adequacy.

Comments: The response is acceptable. Resolved.

9. **FDA Question 14:** *In your AFIA Amendment response received December 13, 2016 in response to FDA Question 34, you provided the document “B. microti AFIA Device Risk Analysis” (Attachment- 33.5_LAB-DSGN-5 .xlsx), which includes analysis of risk for several topics including device safety and human factors. Using a spreadsheet with filtering is an excellent method to capture and explore risks with use of your device and we encourage you to leverage this method.*

You have identified a number of relevant hazards, but you have not drilled down to the level of individual hazardous situations and harms for these hazards. For example, H82 (Babesia microti AFIA BLA-37) lists “Complex instructions or user interface using software leading to incorrect assay procedure.” There are a number of possible causes and hazardous situations that could lead to harm, but you have presented them as a whole rather than exploring each individually. From the list of countermeasures listed, it is clear that you have identified several possible problems that could occur and have likely already performed this analysis, but you have not captured the individual details. Mitigations for H82 appear to include both protective measures and information for safety, and should be assessed and presented individually. It is impossible to determine which mitigations apply to which issues.

In several places, your “potential causes” column has some “harm” information mixed in. If more than one “harm” could occur (e.g., incorrect results and invalid results are often associated with different types of harm with often different severity levels), you should have a separate row for each harm because the severity rating is applicable to each harm, not to each hazard. For example, for H82, you have listed both “incorrect results” and “invalid results” in this single row, although the possible harms associated with these two hazards are often different. “Incorrect results” and “invalid results” likely represent several different risks and each should be analyzed and addressed individually. You will also have separate entries for different hazardous situations if the probability factors are different for each (i.e., likelihood of a hazardous situation occurring and the likelihood of the hazardous situation leading to harm).

In your “Review hazards & risk” tab in column D, you combine “Hazard” and “Risk” when these are actually two different concepts. This should naturally resolve itself by ensuring each risk has its own row. Creating a unique column for “Harm” will also allow you to decouple harm from “Potential Cause” and better identify individual hazardous situations that could lead to harm.

Performing your risk activities at this level allows you to fine-tune how and where you address risk reduction activities in your design, and ensure you have considered different ways harm could occur. In many instances, you have combined them into the same entry and have lost the ability to ensure that each risk is dealt with optimally. It can be difficult to identify the overall reduction in risk without considering them individually. This can be misleading because if you haven't explicitly listed specific causes or situations, it is difficult to ensure that you've identified and implemented the appropriate mitigation(s) (countermeasures) for each of those situations. Using spreadsheet filtering will allow you to quickly see the impact of a particular mitigation or the scope of a particular harm or hazard. Finally, when you are assessing the post-mitigation risk, you do so based on each mitigation individually, which you have not done.

- a. *There are a number of references to the (b) (4) software in this document, although it is not clear how these risks are related to the risk information in the (b) (4) Risk Analysis (Attachment- 34.1_IT-CSV-PDF-41.xlsx), or how traceability is maintained between this and (b) (4) design control documentation. Please explain how the (b) (4)-related information between these two documents is aligned, and how traceability to the requirements is captured.*
- b. *Please provide an update to this risk analysis to identify for each hazard, a list of possible harms, and the hazardous situations/causes that could allow each of those harms to arise from that hazard. Each should be in a unique row. This is necessary to understand the range of possible hazardous situations and to understand how your mitigations reduce each risk to acceptable levels. This will allow a one-to-one mapping with the individual mitigations and more appropriate assessment of the post-mitigation risk. It will also allow you to filter the table looking for trends and assess the impact of different factors, such as the importance of some mitigations or causes.*

Response: In the Amendment received March 20, 2017 (AFIA Information Request Response.pdf), in response to FDA Question 14, the applicant stated that the risk analysis was updated to better align with ISO 14971, and provided an update risk analysis table "Babesia microti AFIA device risk analysis" (Attachment_13.1-LAB-DSGN-5.xlsm). Some changes were made to the risk table, although some changes were not consistent with ISO 14971. Many causes and hazardous situations are not uniquely specified, individual mitigations are not mapped directly to causes, and no traceability is provided for mitigations or testing.

Comments: The response is inadequate. Additional information is required. The following were sent to the applicant in the AFIA Complete Response letter sent June 13, 2017 as FDA 14:

Risk Analysis and Traceability: *In the Amendment received March 20, 2017 in response to FDA Question 14, you provided document "Babesia microti AFIA device risk analysis"*

(Attachment_13.1-LAB-DSGN-5.xlsm). In the “Review hazards & risk” tab, your risk information is presented generally, without specifics. You have not established clear one-to-one traceability between specific potential causes and hazardous situations and the “Countermeasures to take.” Many of the countermeasure entries include several individual countermeasures, and it is not clear how these countermeasures would be adequate to mitigate the potential causes, because the potential causes are not specific. For example, H80 lists several potential causes related to mistakes in manual stages in manufacturing, but you have not explicitly listed the types of mistakes that could be made, the possible harm (severity) of each mistake and the probability associated with each. This should be done, so you can identify the appropriate countermeasures for each.

Please provide additional specifics for each cause/hazardous situation that could occur, and provide countermeasures and pre/post risk assessment for each one. This should capture specific situations, how these situations could come about, and how you address each. For example, if a warning is to be placed in the operator’s manual to address an identified risk, a reference for the explicit warning would appear in your risk documentation for that particular situation. If the information is contained in a manual or SOP, a specific reference within that documentation should be provided. This is necessary to understand that you have identified and considered specific situations that could lead to harm, and identified, implemented and tested mitigations to reduce these risks to acceptable levels. We expect to be able to trace from the identified situations to the specific warnings or guidance you provide as a countermeasure.

Response: In the amendment received October 10, 2017 (001_BL125589 AFIA Imugen Complete Response.pdf) in response to FDA Question 14 on page 25, the applicant stated that the AFIA risk assessment was revised according to ISO 14971 and the new risk management procedure. The applicant stated that the AFIA risk assessment was available for onsite review. Since FDA will not perform an onsite visit before licensure, the document is necessary for review now.

Comments: The following was sent to the applicant on November 30, 2017 as new FDA Question 1:

In the amendment received October 10, 2017 (001_BL125589 AFIA Imugen Complete Response.pdf) in response to FDA Question 14 on page 25, you stated that the AFIA risk assessment is available for onsite review. Please provide this. This is necessary to review the adequacy of the revision you performed.

Response: In the amendment received December 4, 2017, the applicant provided the AFIA risk assessment (001_Attachment-1_LAB-DSGN-5 _AFIA Risk.xlsm). The assessment is significantly longer because the applicant separated each of the individual risk control measures into a separate row to assess individually. This is acceptable. However, the severity levels appear to be assigned incorrectly, and the “residual risk” column was

removed. This results in 13 of the 796 risk rows being reported as “Not Acceptable.” The applicant needs to address these issues, as described in the deficiencies below.

Comments: The following issues were discussed with the applicant during a telecon on December 5, 2017, although these deficiencies were not provided verbatim. The applicant agrees that these issues exist, and we will work interactively to update the AFIA risk assessment and associated process.

In the AFIA risk assessment documentation provided December 4, 2017 (001_Attachment-1_LAB-DSGN-5_AFIA Risk.xlsm), residual risk no longer appears in the risk table, and we are unable to reconcile how you calculate or record residual risk. Your risk table shows 13 risks that remain Not Acceptable after mitigation. The assessment is significantly longer than the previous risk table because it appears you separated each of the individual risk control measures into a separate row to assess individually. This is acceptable. We believe that you are somehow combining the effect of several risk mitigations together because you periodically include a grey row with “Summary of above countermeasures” in the “Risk Controls” column. However, your new Risk Procedure (LAB-QA-62) states that residual risk is to be added to the Product Risk Analysis record, but it does not clarify how to combine the individual risks from the risk table to produce the residual risk. Even though some rows indicate that the risk controls are a “summary of above countermeasures,” the formula for the calculation of those summary row values does not appear to include any risk information from the other rows they are supposed to summarize. Finally, at least one “summary” row has a post-mitigation assessments of “Not acceptable” (e.g., Sequential ID 725). Please clarify how you calculate residual risk, what the “summary” rows indicate, and how final risk levels of “Not acceptable” are to be interpreted. This information should be included in your risk process or risk documentation to aid in interpretation.

It appears that an error exists between your definition of Severity in the “Front page” sheet and the assignment of Severity values in the “Review Hazards” sheet. Several Hazard IDs are associated with a potential harm of death and are assigned a Severity of ‘4’ although “death” is assigned a Severity value of ‘5’. The Severity values should be corrected and the risk table updated.

Response: In Amendment 33 received December 19, 2017 in response to December 5, 2017 telecon, the applicant provided the updated AFIA Device Risk Analysis (002_Attachment-2_LAB-DSGN-5.xlsx). Risks associated with severity of death were properly upgraded to Severity ‘5’. For risks where more than one mitigation exists, the applicant clearly identified the summary row that captures the combined effect of all mitigations, and documented the procedure for how to determine the combined probability and risk levels in the updated Procedure for Product Risk Management (001_Attachment-1_LAB-QA-62_DocDetails.pdf) in section 6.3.1.9. The residual risk column has been restored to the table. All of the identified issues have been resolved.

Comments: The response is acceptable. Resolved.

Note: the comment below also belongs to this long Interactive Question, although it now appears out of place, due to the extensive interactions for this risk-related question.

Comment: The following was sent as additional information to assist in educational efforts related to risk management on April 14, 2017. No response was required.

Additional Information on Risk Documentation and Processes: We recognize your effort to improve your approach to risk analysis and encourage you to seek additional opportunities to continue this effort. We understand that effective risk management can be challenging, and have prepared our comments to encourage your continued efforts in this area. You have included references to both ISO 14971 and FMEAs and the risk tables you provided contain a mix of terminology and concepts.

Because you stated that your processes align with ISO 14971, please consider the following references. Note that much of TIR 32 has been incorporated into IEC 80002-1, although there remain some unique discussion sections on software risk management within the software life cycle that are not included in IEC 80002-1.

- AAMI TIR 32: Medical device software risk management
- IEC 80002-1: Medical device software - Part 1: Guidance on the application of ISO 14971 to medical device software

You might also find TIR 24971 useful in your understanding of ISO 14971.

- ANSI/AAMI/ISO TIR 24971 Guidance on the application of ISO 14971.

You might find value in some industry publications related to the risk management process. Please consider the following from AAMI (Association for the Advancement of Medical Instrumentation). Note that these articles were part of the public discourse at the time seminal industry standards were being formulated or revised, and should be viewed as information and not construed as regulatory requirements. If you do not have subscription access, you may be able to locate articles online or by contacting the authors directly.

- The goal of the following is to provide an understanding of risk management principles to developers of medical device software: Jones, P., Jorgens, J., Taylor, A., Weber, M., Risk Management in the Design of Medical Device Software Systems, Biomedical Instrumentation & Technology Journal, Volume 36, Number 4, July/August 2002.
- AAMI Horizons produced an issue focusing on Risk Management, and the link below includes a link to the Table of Contents.
<http://www.aami.org/productspublications/horizonsissue.aspx?ItemNumber=1954>

Cybersecurity considerations are becoming a larger and larger concern for systems that allow connectivity to the outside world; for example, by way of a network, external storage device, and/or user interface. Some manufacturers include cybersecurity risks in their risk documentation directly, while others perform separate risk management activities for cybersecurity considerations. It is your choice, although you should consider security-related causes to the hazardous situations you identify. Please refer to the following FDA guidance documents, including section VI “Medical device cybersecurity risk management” in the postmarket guidance for a discussion on risk management specific to cybersecurity.

- “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff,” issued October 2, 2014 and available at <http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf>.
- “Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff,” issued December 28, 2016 and available at <https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf>.

Note that there are subtle differences in risk management for cybersecurity, which may complicate the traditional ISO 14971 approach. Because your goal is to be aligned with ISO 14971, you might consider the following popular reference in this area:

- AAMI TIR57 “Principles for medical device security—Risk management”

Note that you many use any number of different methodologies to identify the possible hazards, harms, hazardous situations, etc., that are relevant for your device. Some applicants provide their fault trees and FMEA tables, while others have created a custom table that allows the capture of all information outlined in ISO 14971. Exactly how you present the information is not dictated, but keep in mind that a goal of the review is to assess the scope of your risk management efforts. To do this, we wish to see the hazards, harms, hazardous situations, causes, and mitigations in a single location, with the premitigation assessment of each risk and the postmitigation assessment of each risk clearly shown. This allows us to determine if your proposed mitigations and their ability to reduce the identified risks are reasonable. Traceability to any requirements that implement risk mitigations and the associated testing should also be included.

The following question was generated in response to information provided in the May 23, 2017, communication to FDA, and sent to the applicant in the AFIA Complete Response letter sent June 13, 2017 as FDA Question 17.

10. **FDA Question 17:** *In the (b) (4) status update received May 23, 2017, in response to FDA Question 1(a), you provided (b) (4) infrastructure details ((b) (4) Infrastructure Details.docx).*

- a. *The (b) (4) database server appears to be running on an unsupported operating system, Windows (b) (4). As of July 14, 2015, Microsoft no longer provides automatic fixes, updates or security updates for this product to protect against harmful viruses, spyware and other malicious software. Your Information Technology Security Policy (Attachment_20.2-IT-SEC-POL-01&DocDetails.pdf) does not provide a process for supporting an operating system when patches are no longer available. Please provide your plan for migrating to a supported operating system. If you do not intend to upgrade, please discuss the additional security risks, how you will identify vulnerabilities and manage the risks of this increased exposure.*
- b. *Please identify the cybersecurity product(s), including version number(s), running on each of the servers and computers identified in the (b) (4) specific infrastructure. Your Information Technology Security Policy (Attachment_20.2-IT-SEC-POL-01&DocDetails.pdf) references two generic product lines but does not indicate how the individual systems are protected.*

Response: In the amendment (001_BL125589 AFIA Imugen Complete Response.pdf) received October 10, 2017 in the response to FDA Question 17 on PDF page 33, the applicant explained that the migration from Windows Server (b) (4) to Windows Server (b) (4) is complete.

(a) The test protocol, test plan and verification reports were provided. The applicant stated all shortcuts to the prior version of (b) (4) were removed, and that all design control documentation was updated to remove references to Windows Server (b) (4). This is adequate, except that references to Windows Server (b) (4) still exist, and should be removed to avoid confusion. See the comment below.

(b) The applicant stated that “[i]n order not to compromise the security of our system and in accordance with IT-SEC-POL-1, “Information Technology Security Policy”, we are not permitted to provide cybersecurity software versions in written communications.” Further, the applicant stated that the information can be provided during the FDA pre-licensure inspection. Nothing in the applicant’s security policy references software versions in written communications. The document only reference to a list “restricted applications” that are maintained by IT and periodically reviewed, and no criteria or definition is provided for what a restricted application is. The applicant should respond to the question.

Comments: The following was emailed to the applicant on November 9, 2017 as new FDA Question 3:

In the complete response (001_BLI25589 AFIA Imugen Complete Response.pdf) received October 10, 2017 in the response to FDA Question 13 on PDF page 34, you stated that the migration from Windows Server (b) (4) to Windows Server (b) (4) is complete. Please address the following:

- a. In part (a), you provided the (b) (4) DB Migration Verification test protocol document (051_Attachment-13.4_IT-(b) (4)-SPT-30& Doc Details.pdf) describing performance of the migration testing but did not provide the results of these tests cases. Only a summary test report was provided (052_Attachment-13.6_IT(b) (4) SPT-31& Doc Details.pdf). Please provide the document containing the results of the test scripts and protocol. This is necessary to confirm completion of the migration testing.*
- b. In part (a), you stated that all references to Windows Server (b) (4) have been removed. Please note that at least one document still references Windows Server (b) (4) and should be updated: (b) (4) Software System Test Plan (024_Attachment-6.4_IT-(b) (4)-1 & Doc Details.pdf). Please check to ensure all documents are correctly updated.*
- c. In part (b), you stated that according to your security policy, IT-SEC-POL-1 (Attachment_20.2-IT-SEC-POL-01&DocDetails.pdf) “we are not permitted to provide cybersecurity software versions in written communications.” We are unable to identify this restriction in your security policy. Please provide this information and clarify the concerns below, as these are necessary to complete the review of your submission. Stating that “(b) (4) software and (b) (4) are implemented on the network” with no further details is not sufficient to evaluate that the vulnerable components of your system are adequately protected, or provide confirmation that the software is running on all computers and servers in the system. If you are not using the latest version of the referenced programs, please provide your assessment that the differences between the version used and the latest version do not adversely impact your system. If you continue to have concerns about providing this information, please submit it via DCC or send an email to SecureEmail@fda.hhs.gov and we will assist you in determining the type of secure communications to establish so that this information can be provided to continue this review.*

Response: In the amendment (001_Response to IR Received 9Nov2017_AFIA.pdf) received November 20, 2017 in response to FDA Question 3, the applicant provided the following:

- (a) The verification was inadvertently omitted, and has been provided. It is adequate.
- (b) The applicant clarified their original statement to indicate that appropriate references will be maintained; for example, references within the migration plan itself. This is adequate.
- (c) The versions of (b) (4) were provided, and the applicant stated that versions are

updated automatically as per policy. At the time this response was prepared by the applicant, both (b) (4) was actually shipping later versions of software.

The following should be conveyed to the applicant:

In the amendment (001_Response to IR Received 9Nov2017_AFIA.pdf) received November 20, 2017 in response to FDA Question 3, you provided the versions of cybersecurity programs in use and stated that these are the latest version released and that you adhere to your policy of receiving automatic updates. Please note that at the time your response was prepared, both programs were currently advertised as having later versions of software than you provided. You should ensure that your mechanism for receiving automatic updates is working correctly. No further response is required.

Comments: The response is acceptable. Resolved.

The following questions are related to both the NAT and AFIA assays but were initiated from the March 23, 2017 CR response to the NAT submission for questions that had been inadvertently left off the AFIA communication. They are relevant to the AFIA submission but are not directly traceable to previous questions due to the oversight.

11. FDA Question 10: User interface error checking (sent as FDA Question 3):

In the NAT Amendment received March 23, 2017, in response to FDA IR Question 15, you stated that two additional risks were added, but it is not clear if this represents all unexpected conditions. Two conditions were included: R26b “Software must protect against import of corrupt or incomplete source file” and R26c “Software must not allow input of invalid result values.” Testing for R26b does not describe what was tested and why; it just illustrates that an uncharacterized file was rejected on import. Testing for R26c is limited to error checking on the IFA Slide screen. R29 describes software error detection functionality but the testing that is included in the traceability matrix (Attachment_15.2-IT-CSV-IMD14-16-TM&DocDetails.pdf refers to IT-CSV-IMD14-07-OPQb, 6.8.11, #11) does not appear to test or detect error conditions.

- a. *Please provide a summary description of all user interface requirements and the types of error checking that is performed to identify problems with data interactions with the user via keyboard, barcode scanning, etc., and list the corresponding testing used to ensure proper functionality of the system. Please do not refer to entire design documents, but develop a direct response to this question. This is necessary to assess how the system responds to unexpected conditions and assess the scope of the error checking of the system.*
- b. *Please provide the corresponding design control documentation for the user interface requirements and error checking in (a).*

Response: In the amendment received October 10, 2017 (001_BL125589 AFIA Imugen Complete Response.pdf) in response to FDA Question 10 on page 14, the applicant provided a detailed list of the modules that require user interface with (b) (4) and summarized the error checking for each. Each software requirement was listed by number, with the corresponding summary of verification testing. This is adequate. However, R29 was not discussed.

Comments: The following was sent to the applicant on November 11, 2017 as new FDA Question 2.

In the complete response (001_BL125589 AFIA Imugen Complete Response.pdf) received October 10, 2017 in the response to FDA Question 10 on PDF page 15, you discussed requirements for error checking. FDA Question 10 stated that R29 describes software error detection functionality but the referenced testing does not appear to test or detect error conditions and no descriptive information was provided. Please clarify the purpose of this test and how it ensures that the requirement was adequately met.

Response: In the amendment (001_Response to IR Received 9Nov2017_AFIA.pdf) received November 20, 2017 in response to FDA Question 2, the applicant stated that “*this requirement addresses the ability to identify altered records through the analysis of audit table queries and is not intended to address software error detection functionality.*” The requirement itself is poorly-written and the associated testing provided are not sufficient to determine if the requirement was adequately met. However, the topic is audit functionality and not (b) (4) functionality, so we will not challenge the applicant’s assertion “*that the requirement was adequately met.*”

Comments: The response is acceptable. Resolved.

12. **FDA Question 11:** *Documentation package for Build 1.0.5.5 (sent as FDA Question 5): In the NAT Amendment received March 23, 2017, in response to FDA Question 14, you stated that the (b) (4) software will no longer be compiled for commercial release, but that the final version will be Build 1.0.5.5. Please review the documentation provided and ensure that all design documentation including appropriate verification and validation testing corresponding to version Build 1.0.5.5 has been provided.*

Response: In the amendment (001_BL125589 AFIA Imugen Complete Response.pdf) received October 10, 2017 in the response to FDA Question 11 on page 19, the applicant provided a table of updated design control documentation for Build 1.0.5.5, and referred to Attachment 13.3, which contains a table of a complete list of design documentation sent to FDA and which documents are obsolete. This is acceptable.

Comments: The response is acceptable. Resolved.

8 Appendix 2: Device Description Details

Network Diagram: The following hardware network diagram was produced to illustrate the components of the system, the boundaries of the system, and the various operating systems and data flows. (023_Attachment-8.1_IT-CSV-IMD14-15-AD &Doc Details.pdf)

2 pages have been determined to be not releasable: (b)(4)