STATEMENT OF WORK
Title: X-ray computed tomography simulation software
Lab: Engineering Laboratory

I. BACKGROUND INFORMATION

NIST CHIPS Metrology R&D program has nondestructive defect detection metrology (NDDM) for semiconductor advanced packaging project. The NDDM project aims at developing simulated data sets to improve X-ray computed tomography (XCT) defect detection metrology and accuracy of detection. An XCT simulation software is acquired to allow generation of data sets simulated at different acquisition settings. The simulation software settings will be validated and compared with physical datasets. The simulated data complements physical data sets to be developed. Simulation allows quicker generation of data sets acquired at different settings. This is critical for improving efficiency and productivity of semiconductor failure analysis process.

II. PURPOSE

The XCT simulation software allows generation of data sets acquired with various scanning trajectories and acquisition parameters.

III. MINIMUM REQUIREMENTS

Line Item 0001: XCT simulation software
Description: Permanent license of simulation software
Quantity: one (1) license

A. Technical Specifications

a. Source
   i. Capable of simulating various vendor's laboratory transmission and reflection laboratory sources and geometries.
      1. A stronger consideration will be given to a software that can simulate synchrotron.
   ii. Capable of simulating X-ray energies from 1 keV to at least 450 keV range.
   iii. Capable of simulating monochromatic and polychromatic spectrum.
   iv. The source spectrum should consider electron beam energy, anode material, thickness, and angle, window material and thickness, and pre-filter.
   v. Capable of adjusting source spot size.

b. Simulation objects
   i. Capable of directly using three-dimensional (3D) surface meshes (e.g., stl file format) for simulation.
   ii. Allows importing custom surface meshes.

iii. Allows integration of multiple mesh objects and materials for simulation.
iv. Allows Boolean operations of the meshes such as union, intersection, or difference.
v. Capability to generate basic shapes (e.g., cylinder, cuboid, ellipsoid, etc.).

c. Scattering
    i. Capable of simulating the effect of scattering through Monte-Carlo or a comparable method.
d. Detector
    i. Considers scintillator material and its detection/conversion efficiency.
    ii. Capable of simulation various detector configuration such as flat panel detector and optical camera-based detector.
    iii. Capable of controlling detector signal-to-noise ratio and image sharpness to make image comparable to experimental measurements.
e. Scanning trajectory
    i. Capable of simulating various scanning trajectory including circular, laminographic, and custom
f. Scripting
    i. Capable of using a scripting language to vary parameters and run simulations.
    ii. A stronger consideration will be given to a software with python-based API
    iii. Allows simulating variations that can occur during scans such as source spot size/position or sample position drifting through scripting.
g. Output
    i. Capable of generating radiographs in typical image format (e.g., tif/tiff file formats).
    ii. A stronger consideration will be given to software with reconstruction capabilities.
    iii. A stronger consideration will be given to a software allowing reconstruction of data generated from a difference source (simulation or physical measurements).
h. Phase contrast
    i. A stronger consideration will be given to a software allowing simulation of phase contrast.
    ii. A stronger consideration will be given to a software with phase retrieval-based reconstruction.
i. License type
    i. One license is required, and the software will be used on a single computer.
    ii. Allow the use of software through Windows remote desktop.

Line Item 0002: XCT simulation software
Description: Maintenance
Quantity: one (1) include the first year of maintenance contract.

IV. SCHEDULE OF DELIVERABLES

Deliverable Number	***Description***	***Quantity***	***Due Date***	***Place of Delivery***
1	One (1) permanent license of XCT simulation software	One (1)	No later than 2 weeks after receipt of order.	Electronic delivery or NIST (Gaithersburg) if a dongle is sent
2	1 year maintenance contract	One (1)	No later than 7 days after receipt of order.	Electronic delivery

Standards of Acceptance: The NIST TPOC shall review all the above deliverables and respond with an acceptance or request for revision email to the Contractor Point of Contact (POC) within 7 days of receipt of deliverable. This section applies to deliverables which must be reviewed and approved for acceptances (e.g., draft plans, drawings, etc.).

V. DELIVERY TERMS

Delivery shall be F.O.B Destination (or equivalent incoterms, such as DDP) and shall occur in accordance with the delivery due dates provided in the below table.

FOB Destination means: The contractor shall pack and mark the shipment in conformance with carrier requirements, deliver the shipment in good order and condition to the point of delivery specified in the purchase order, be responsible for any loss of and/or damage to the goods occurring before receipt and acceptance of the shipment by the consignee at the delivery point specified in the purchase order; and pay all charges to the specified point of delivery.

The contractor shall deliver all Line Items to:
National Institute of Standards and Technology
Shipping and Receiving
100 Bureau Drive, Building 301
Gaithersburg, MD 20899
TBD, Building 233

VI. PAYMENT SCHEDULE

100% after delivery and acceptance by the POC of fully installed software.

VII. CYBERSECURITY PRIVACY REQUIREMENTS

NIST seeks a solution that provides security and privacy protection consistent with requirements defined by applicable federal laws, regulations, policies, and standards (e.g., the Federal Information Security Management Act (FISMA), OMB Circular A-130, and FIPS Publication 200). The solution provider (including subcontractors) may meet these requirements through various means, including but not limited to FedRAMP authorization, current third-party assessments (e.g., SSAE, PCI), and/or responses to NIST special publication control set SP 800-171.

Minimally Acceptable Controls

- System security plan describing physical, technical, and administrative controls implemented to protect systems and sensitive personally identifiable information (SPII).
- IT management processes to establish and manage secure configuration baselines including routine patching for all operating systems and applications.
- Access to SPII is restricted to those with a need to know. Personnel with access to SPII have background investigations performed (e.g. criminal, financial etc.), and are trained on secure handling of SPII.
- Access Controls for SPII meet or exceed industry best practices for access and identification control including, but not limited to, connectivity to servers and databases, multi-factor authentication for remote accesses for administration, secure configurations for any devices accessing the system, and strong physical security for any place where the data is accessed.
- The solution supports multifactor authentication for users and/or supports integration with customer federation services for Single-Sign capability.
- Processes for scanning on a continual basis for vulnerabilities and proper configurations for all aspects of the system, as well as processes for timely mitigation of findings.
- Auditing and Incident Response processes including customer notification of suspected or actual incidents and logging with sufficient information to perform forensics on any incident. Processes for notifying and providing appropriate mitigations, including but not limited to credit monitoring services, for subsidy applicants in the event of suspected or actual incidents.
- SPII is encrypted in transit using TLS 1.2 or better and encrypted at rest in all places the SPII is stored. All encryption algorithms and modules are FIPS 140-2/140-3 validated.

If unable to meet any of the requirements listed above, the solution provider may provide details of mitigations or alternative protections in place to ensure the appropriate handling and protection of SPII.

If the solution provider provides services to other Federal agencies, provide a general description of the security risk management approach and client point of contact.