ANNEXURE A

EXTRACT FROM INFORMATION AND CYBER SECURITY IMPLEMENTATION GUIDE SECTION 10 – APPLICATION DEVELOPMENT AND ACQUISITION TABLE 10-1

SyDLC PHASE	PROCESS	DESCRIPTION OF ACTIVITIES
1. **PLANNING -** The initiation phase ensures that the system is correctly planned to address the security requirements of the organization.	Security Planning and Risk Assessment	Perform Security Planning and Risk Assessment with a focus on the following: • Appoint the Information Security Officer or the person in charge of the subject of IT. • Appoint a Information Security expert to the Technical Evaluation Committee (TEC). • Determine the Classification of the System following a risk assessment of the proposed system and Identify information security requirements of the organization with the active involvement of Information Asset Owners/Process owners and ISC, and document requirements. • Based on the risk assessment, & reuqirements of the government orqanization, TEC is responsible for identifying appropriate controls to provide appropriate protection to the proposed system.
2. **ACQUISITION -** Based on organizational requirements (including information security requirements), an application is developed/procured.	Tender Security Requirements	• Define and Document Security Requirements in the Tender document and Evaluate the Bids • The TEC develops Technical Specification of the proposed system by considering information security requirements of the organization. In addition to the security requirements, specific security requirements that are to be followed in line with the applicable policies, guidelines, standards (e.g. ISO 27000, PCI DSS) shall be followed. • The organization should keep the rights to audit the system. The organization shall have the right to audit the source code, architecture, library modules or any other features/functions of the proposed system. However, in a situation

		where such rights cannot be obtained for the organization, assurance shall be obtained through a third-party auditor that the security requirements specified in the design are met and secure coding standards are being incorporated into the application code by vendor. • Upon the receipts of Bids (Tenders which include the technical proposal) the TEC shall evaluate the bids by assessing of security controls/architectures proposed by the Bidders. • Technical Evaluation Report is prepared by TEC.