State of California

Department of Technology

Questionnaire for Information Security and Privacy Components in Feasibility Study Reports and Project-Related Documents

SIMM 20D

June 2014

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	**July 2008**	**Office of Information Security & Privacy Protection**	
Update	**March 2011**	**Technology Agency - Office of Information Security**	**Formatting, name and logo change.**
Update	**April 2011**	**Technology Agency - Office of Information Security**	**Formatting and SIMM Numbering**
Update	**June 2014**	**Department of Technology – Office of Information Security**	**Department of Technology name changes**

Table of Contents

Questionnaire for Information Security and Privacy Components in Feasibility Study Reports and Project-Related Documents

1.0 INTRODUCTION

The following Questionnaire assists Agencies/state entities with describing the information security and privacy components associated with an IT project in its Feasibility Study Reports and other project-related documents. The Office of Information Security reviews these documents to ensure information security and privacy components are addressed by the Agency/state entity and provide its recommendations to the California Department of Technology (Department of Technology).

If any of the answers could be considered sensitive in nature, the Agency/state entity should address them in a separate addendum marked "Confidential" and included as an attachment to the document.

2.0 INFORMATION SECURITY OFFICER (ISO) ROLE AND RESPONSIBILITIES

1. What is the role and responsibilities of the Agency ISO in relationship to this project?
2. Will the ISO be involved in developing and reviewing the security requirements?
3. Will the ISO be involved in developing and reviewing the security testing efforts?
4. Has the ISO participated in the response to these questions and signed off on the project-related document(s)?

3.0 PROPOSED SYSTEM

1. Who will be the designated owner of the proposed system (system)?
2. Who will be the custodians and users of the system?
3. Has the data for the system been classified by the owner? Explain.
4. Does the project require development of new application code or modification of existing code? Explain.
5. Will your Agency/state entity share the data for the system with other entities? If so, who?
    a. Federal partners
    b. Local city/county partners
    c. State agency partners
    d. Judicial branch
    e. Universities
    f. Researchers
    g. Others
6. If data for the system is to be shared with other entities, will your Agency/state entity implement data exchange agreements with the entities? Explain.
7. Are there checkpoints throughout the software development life cycle (SDLC) verifying and certifying that the security requirements are being met?
8. At what points will risk assessments be performed throughout the SDLC?
9. At what point will vulnerability assessments be performed once the system is put into production (e.g., ongoing risk management after implementation)?

10. Will this system collect federal data? If so, have you yet determined the National Institute for Standards and Technology 800-53 rating (i.e., high / medium / low)?
11. Does your Agency/state entity's IT Capital Plan address information security and privacy as related to this system?