CGI CA—> CAREMAIL PROJECT

SECURE DEVELOPMENT SUPPLEMENT

TABLE OF CONTENTS

1 DESIGN CONSIDERATIONS

During the development of initial application specifications, the security and privacy attributes of the application are identified and documented. Formal guidelines may be used to help identify security and privacy expectations and create a risk-based approach to security controls that are embedded in the architecture and deployed in the infrastructure. Common guidelines and standards including those described by NIST Special Publications (NIST SP 800 series), SANS, ISO, COBIT and other frameworks are considered. In many instances, application specific [i.e. Children's Online Privacy Protection Rule ("COPPA")] and industry or government security requirements are suggested or mandated. The application sponsor is consulted and, if necessary, provided with a summary of the value and benefits of each so that the standards and controls most relevant to the application can be selected.

In addition to the selection of the applicable set of controls, design considerations are documented that are instrumental in creating an architecture that is secure, resilient, efficient and meets all the expected operational requirements.

During the design stage, consideration is given to enhancing security in the following areas:

- Role based Authentication – restricting the functions available to users based on their expected authority and function.
- Sensitive Data Consolidation – design of a database that has mixed data sensitivity so that data with similar protection attributes are stored in tables or data area that can be controlled separately and even physically stored apart from data with other protection attributes.
- Creating detailed activity logs so that all attempts to access, change, or delete sensitive data is recorded and can be retrieved for review upon demand or, in the case of personal privacy data, returned upon valid request of the individual.
- Preventing or limiting replication, relocation or destruction of data without proper process and within appropriate compliance requirements.

Common services are created or re-used as available for shared security functions such as user authentication, role authorization, data validation and notifications. Particular attention is given to:

- Accurately determining the identity of the individual and retaining the proper control so that authentic identity is established upon initial account access and retained and protected on an ongoing basis. Techniques include multi-factor authentication that requires entry of more than one of the following: 1)what you know, 2)what you have, and 3)what you are. This can require the application to use biometrics, tokens or correct answers to personal questions among other techniques.

- Data encryption is a common industry standard for preserving data privacy. Encryption products are considered along with the encryption key management process for recovering encrypted archives or data encrypted by former employees or partners.
- Understanding privacy assertions, constraints, and uses of personal data is a consideration on many applications. Communication of understanding and accepting them, along with agreeing to appropriate use, is a common design element in public access systems.

Security, privacy, and compliant architecture are key expectations of the design stage of CGI's security application development methodology.

2 DEVELOPMENT CONSIDERATIONS

Application development, particularly in the internet environment is an evolving technology. The constant threat of increased malicious attempts by organized criminals and agents requires constant vigilance and an effective process for implementing mitigation efforts against threats. Application code vulnerabilities are being constantly discovered and are made available by public and private research organizations to secure development organizations. CGI uses these research organizations to evaluate that code under development is using all appropriate methods to minimize the opportunity to exploit these known vulnerabilities.

Before all application source code is accepted, it is scanned using at least one robust static code scanning utility that is focused on finding coding weaknesses. All online application program modules are developed in accordance with the Online Web Application Security Program ("OWASP") expectations and tested to identify and eliminate the SANS Top 10 source code vulnerabilities.

3 TESTING CONSIDERATIONS

Before production acceptance and periodically, operational applications are evaluated using a dynamic vulnerability scanning process that employs a "penetration test" or attempt to break into the application without authorization, and a persistent threat detection process that emulates a step-by-step attempt to breach security defenses in ways that approximate the procedures used by organized malicious “hacker” groups.

4 OPERATIONAL CONSIDERATIONS

During operation, the application environment is constantly evaluated for the immediate detection of malware before it can establish itself. This is done using: frequently updated anti-virus scanning software; security incident and event management (“SIEM”) facilities that discern security breach attempts before they are successful; and constant replication of all databases, application code, and parameters in a remote location. The latter is done so recovery from data center disruptions is swift and accurate with little or no loss of data, even the transactions in process.

Constant monitoring of the infrastructure assures that changes are authorized and approved, patches and updates are scheduled, tested and controlled and hardware components are kept safe from disruption, damage or unapproved alteration.