C-Level Security
STRATEGIC SOLUTIONS

39506 N. Daisy Mountain Dr.
Suite 112-225
Phoenix, AZ 85086
480-703-7975

To the Management of SurePrep, LLC:

C-Level Security, LLC has validated the SurePrep assertion, for the mobile iOS and Android application named **"TaxCaddy™", providing services from 1 October 2018 through 30 September 2019**, the "SurePrep TaxCaddy™" team and has developed, deployed, and has shown to actively maintain effective security controls, to provide reasonable assurance that the application:

- Was available for operation and use as defined in the license agreement;
- Implemented controls to help protect against unauthorized physical or logical access;
- Protected information that was designated as confidential as committed or agreed; based on safeguarding requirements under Graham Leach Bliley Act and applicable corporate policies;
- Limited exposures of data on the devices when not in use.

This assertion is the responsibility of SurePrep's management. Our responsibility is to express an opinion based on our review and assessment of controls implemented during the testing of said system(s). Our examination was initiated in June and is re-tested on an ongoing schedule and, accordingly, included (1) obtaining an understanding of relevant security, availability, processing integrity and confidentiality controls, (2) testing and evaluating the operating effectiveness of control; and (3) performing such other procedures as considered necessary in the circumstances. Examination was conducted from an authenticated and unauthenticated role, utilized automated and manual testing techniques, source code review (where applicable), and engineering discussions. Items identified as posing risk were mitigated or resolved based upon an agreed upon schedule and were verified as such through regression testing.

We believe our assessment provides a reasonable basis for our opinion. Because of inherent limitations in application dependencies, error, fraud, or dependencies to supporting systems such as networks and operating systems no controls can provide one hundred percent assurance of system security. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls supporting the system, the failure to make needed changes to the system or controls based upon a newly discovered security vulnerability, or a failure to follow stated and defined controls supporting SurePrep system operations.

In our opinion, SurePrep's management assertion, referred to above, is fairly stated in all material respects. The C-Level Security Certified Seal on the SurePrep site constitutes a symbolic representation of the contents of this report and should not be interpreted to supersede this report.

Clinton Mugge
President
C-Level Security, LLC
September 27, 2018

39506 N. Daisy Mountain Dr.
Suite 112-225
Phoenix, AZ 85086
480-703-7975

Company Overview

C-Level Security has been providing information security consultancy and training for many recognizable Fortune 100 level organizations since its origination in December 2004. C-Level Security believes in the process of operational driven information security needs flowing freely between IT and Management. C-Level Security consultants and trainers have deep pedigrees in many of the top information security companies such as Foundstone, Accuvant, and Mandiant, along with various Big 4 accounting firms and US Armed Services.

The C-Level Security Professional Services Team has developed a cohesive, interwoven, step-by-step process that is employed for each customer on every engagement so our strategic solutions today can enhance your organization tomorrow. From Requirements to our Ongoing Commitment, our service delivery expertise targets a continuous goal of imparting leading security practices for tactical and strategic improvement. Our "sweet spot" is on delivering solutions addressing the broad spectrum of regulatory and compliance requirements, threats, risks, and infrastructure needs. Our team is comprised of security and compliance professionals that hold CISSP, CISM, and CISA credentials.

C-Level Security Professional Services benefit our customers by building on core principles:

- **Personalizing** to your unique enterprise culture creating smoother workflow and ongoing commitment
- **Integrating** your requirements and best practices to create defined objective criteria
- **Extracting** true business risk from traditional technical risk in order to communicate to an executive audience
- **Remediating** findings is executed by your team through detailed recommendations
- **Creating** a security roadmap to address systemic issues and reduce future exposures based on findings

39506 N. Daisy Mountain Dr.
Suite 112-225
Phoenix, AZ 85086
480-703-7975

Overview of Assessment Scope

A high level description of each review component performed is outlined below:

Design and Threat Modeling Assessment

Design and Threat Modeling was performed with business teams, engineering teams and operational teams (system, database, and network). This was performed via discussions and review of documentation pertaining to the specific application, as well as weighing input from SurePrep regarding the application requirements set forth during the development process.

Discussions focused on the user model, user case scenarios, application components, application dependencies, the dataflow model and the controls present on each communication point. Using the model of least privilege C-Level Security assessed the means used to secure the information during entry, transmission and storage items beyond what an external 'black box' application assessment accomplishes.

Application Security Assessment

Application Security Testing involved both "black box" and "white box" review of the application, functions and dependencies. The testing leveraged automated scanning as well as manual testing. While automated scanners provide some security coverage they effectively address only 35% to 40% of security risks. Categories of testing and a brief description are provided below in Table 1.0 Tested Categories. During each of the testing phases, security consultants examined two attack scenarios: unauthenticated and authenticated users. An unauthenticated user is anyone on the Internet who does not possess valid credentials for the application. An authenticated user is anyone who holds valid login credentials. Authenticated users can carry out any of the functions of an unauthenticated user, plus more specific functions within the application depending on the user's specific level of privilege.

.

Category	Description
Input and Data Validation	Is the input your application receives valid and safe? How does your application filter, scrub, or reject input before processing.
Authentication	Are you the user? The process where an entity provides some validation of identity, typically through a user name and password.
Authorization	What rights do you have? Process by which the application provides access controls for resources and operations.
Configuration Management	How does the application run? What databases does it connect to? How is administration performed? How are these settings secured? Refers to how your application handles these operational issues.

39506 N. Daisy Mountain Dr.
Suite 112-225
Phoenix, AZ 85086
480-703-7975

Sensitive Data	Is there sensitive data and how is it protected? Sensitive data is data that must be protected either in memory, over the network, or in persistent stores. What controls protect this data?
Session Management	How do you manage user sessions? How does the application control access of an authenticated user to authorized activities viewing only their sensitive data?
Cryptography	How do you protect confidentiality in transit and storage? Cryptography refers to enforcing confidentiality and integrity of the data.
Parameter Manipulation	How are parameter values handled? Fields in forms, query arguments, and cookies are frequently used to pass parameters for an application. How does your application safeguard tampering of these values? How does the application process input parameters?
Exception Management	When the unexpected happens how does your application respond? Do you limit errors? What do you tell end users? Does your application fail open or closed? Does the way it fails protect the application?
Auditing and Logging	Who When and Where. Auditing and logging refer to recording security-related events.

Table 1.0 Categories Tested

Network Infrastructure Review

The Network Infrastructure was reviewed from both a "black box" perspective using network vulnerability scanners. The scans performed against the deployed environments focused on determining if vulnerabilities were present in production deployments. These tools performed the following functions against the deployed network and available services allowed through the network:

- Listening network services and OS fingerprint
- Remote service versions and configuration
- Information that can be enumerated remotely
- Remotely accessible vulnerabilities