February 18, 2021

Veracode, Inc.
65 Network Drive
Burlington, MA 01803
United States

IDM Computer Solutions
5559 Eureka Dr
Ste B
Hamilton, OH 45011
United States

To whom it may concern:

This letter summarizes activities performed by Veracode in assessing the security posture of the **UltraEdit** application.

Veracode is the only independent provider of cloud-based application security verification and intelligence services delivering unbiased proof of application security to stakeholders across the software supply chain. The Veracode platform provides the fastest, and most comprehensive solution for improving the security of internally developed, purchased or outsourced software applications and third-party components. Offered as a Software-as-a-Service (SaaS), Veracode uses its award-winning, proprietary *static* and *dynamic* analysis technologies to test software applications for security flaws and vulnerabilities, reporting detailed actionable findings and remediation guidance.

Veracode's patented *static binary analysis* technology inspects software executables (compiled binaries or bytecode) for security flaws without requiring customers to provide their intellectual property in the form of source code. By examining a compiled form of an application, static binary analysis can provide a more comprehensive picture of real-world vulnerabilities with a lower false positive rate. Through advanced modeling, Veracode's static engine detects flaws in the software's inputs and outputs that cannot be seen through penetration testing alone. Specifically, Veracode's binary analysis creates a behavioral model by analyzing an application's control and data flow through executable machine code - the way an attacker sees it. Unlike source code review tools, this approach accurately detects issues in the core application and extends coverage to vulnerabilities found in 3rd party libraries, pre-packaged components, and code introduced by compiler or platform-specific interpretations. Binary analysis can also detect other threats, such as those coming from malicious code and backdoors – which are difficult to spot with traditional tools because they are not visible in source code.

Your organization has determined that the **UltraEdit** application has a **Very High** business criticality. For most customers, applications with a Medium or higher business criticality indicate applications that are mission critical for the organization. As such, for the **UltraEdit** application, Veracode conducted the following automated security assessments, employing the techniques outlined above:

Analysis Type: Static
Analysis Date: February 18, 2021
Scan Name: 16 Feb 2021 Static

Summary of the final findings, after mitigations:

Flaw Severity	Flaw Count
Very High	0
High	0
Medium	19
Low	196
Very Low	0
Informational	28

Note of Qualification:

- This degree of assurance provided by any assessment is contingent on: (*i*) the integrity of information provided by the organization during the assessment process; (*ii*) the organization's willingness to allocate the resources necessary to execute a level and scope of assessment appropriate to the security characteristics of the application and the sensitivity of information assets in the environment, (*iii*) the organization's execution of recommended remediation measures.
- No methodology definitively proves the absence of vulnerabilities.
- Following assessment and remediation, modifications to an application, its platform, network environment, and new threat vectors may result in new application security vulnerabilities.