LUMEN SECURITY BRIEF

Nick Coult, Vice President, Interactive Intelligence Systems
Numerica Corporation
nick.coult@numerica.us, 970-207-2252

The security of law enforcement data is paramount. In order to protect such data from inadvertent disclosure or unauthorized use, Lumen is designed to satisfy the requirements of the FBI Criminal Justice Information Systems (CJIS) Security Policy[1]. This document gives an overview of the security measures put in place in order to comply with the CJIS policy and protect critical customer data. Please contact Numerica for additional details.

Access. Access to Lumen is restricted to law enforcement personnel specifically authorized by their agencies to use it, and to cleared Numerica employees for the purpose of maintaining and supporting the software.

All Numerica employees with access to Lumen are subject to the screening and training requirements of the CJIS Security Policy. These employees are fingerprinted and subject to a criminal background investigation by the Colorado Bureau of Investigation (CBI), and must periodically complete CJIS training offered by CBI. Furthermore, each such employee is required to sign and submit the FBI CJIS Security Addendum Certification.

Authentication. All logins to Lumen must comply with the authentication requirements of the CJIS policy. Lumen implements *advanced authentication* for all users, regardless of their location. Advanced authentication in Lumen is accomplished in one of two ways:

[1] http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view

- *Client SSL certificates.* Numerica generates a unique cryptographically-signed certificate for each user, which they must install on their computer or mobile device. When attempting to log in to Lumen, in addition to this certificate, the user must have a valid login and password to access Lumen.
- *Two factor authentication.* Users can opt to register a cell phone or smart phone as a two-factor authentication device. When logging in to Lumen, in addition to the login and password, the user must confirm using their registered device that the login is authorized.

Auditing. Certain events, including password changes, failed login attempts, and other security-related events, are logged in our data center and available for audit for a period of one year, as per the CJIS policy requirements. Lumen customers can request audit logs at any time.

Encryption. All data in transit between Lumen's servers and customers is encrypted. Lumen's software and servers employ encryption software and algorithms that meet the FIPS 140-2 standard as required by the CJIS security policy.

Physical Security. Lumen's secure data center is accessible only to authorized, CJIS-cleared Numerica personnel and is protected by a 24/7 monitored alarm system. Additionally, it is supported by redundant power, cooling, and Internet access points for improved reliability.