BIO-key™
Revolutionizing Authentication

FBI Cyber Task Force Advises Businesses to Incorporate Biometric Factors to Mitigate Multi-Factor Authentication Risk

Warns Mainstream Token and Phone-Based Multi-Factor Approaches are Vulnerable to Circumvention

Wall, NJ, October 10, 2019 - BIO-key International, Inc. (NASDAQ: BKYI), an innovative provider of biometric authentication and security solutions, today said several media reports announced that the FBI Cyber Task Force recently issued a four-page Private Industry Notice that recommends the addition of biometric factors and behavioral information checks to multi-factor authentication (MFA) approaches, citing known and exploited vulnerabilities of token and phone-based multi-factor authentication methods.

The FBI's notice, issued as part of National Cybersecurity Awareness Month, provides important validation for the use of biometric hardware and software authentication solutions such as those developed by BIO-key. The FBI's report has received broad media attention including Forbes, ZDNet and BankInfoSecurity.com. BIO-key's authentication solutions are unique in the market in that they allow interoperability among over 30 different fingerprint scanners from a variety of manufacturers and are available as a turnkey Windows Active Directory authentication solution for enterprises, as well as an authentication platform module ready to serve our federated IAM partners' customers.

The FBI reported that a large variety of schemes and attacks are being used by cyber actors to defeat multi-factor authentication, including social engineering, SIM swapping and account-takeover malware such as Muraena and NecroBrowser.

The FBI's mitigation recommendations are simple:

- Educate users and administrators to identify social engineering trickery.
- Consider using additional or more complex forms of multi-factor authentication for users and administrators such as biometrics or behavioral authentication methods.

The FBI recommendation comes after its review of victim reports to the Internet Crime Complaint Center and actual criminal attacks against mainstream multi-factor authentication methods. The notice marks the first time since 2015 that the FBI has expanded upon its initial recommendation to use multi-factor authentication.

"The FBI's report and recommendation is so powerful because it comes from their unique vantage point from the front lines, fighting cybercrime and investigating real breaches, not from an ivory tower or hardware token industry standards group," said Jim Sullivan, BIO-key's SVP of Strategy and Compliance. "The FBI has one goal, which is the prevention of cybercrime, and that makes them a very credible source," Sullivan added.

“Biometrics should not be an afterthought in a comprehensive Identity Access Management (IAM) strategy,” said Mike DePasquale, BIO-key CEO. “It should be a core design factor in an IAM platform, for end-user authentication, provisioning and governance. BIO-key offers our customers a comprehensive set of biometric authentication options, both on-device and on-server, to meet the real needs of business users,” continued DePasquale.

About BIO-key International, Inc. (www.bio-key.com**)**
BIO-key is revolutionizing authentication with biometric solutions that enable convenient and secure access to information and high-stakes transactions. We offer alternatives to passwords, PINs, tokens, and cards to make it easy for enterprises and consumers to secure their devices as well as information in the cloud. Our premium fingerprint scanning devices offer market-leading quality, performance and price.

BIO-key Safe Harbor Statement
All statements contained in this press release other than statements of historical facts are "forward-looking statements" as defined in the Private Securities Litigation Reform Act of 1995 (the "Act"). The words "estimate," "project," "intends," "expects," "anticipates," "believes" and similar expressions are intended to identify forward-looking statements. Such forward-looking statements are made based on management's beliefs, as well as assumptions made by, and information currently available to, management pursuant to the "safe-harbor" provisions of the Act. These statements are not guarantees of future performance or events and are subject to risks and uncertainties that may cause actual results to differ materially from those included within or implied by such forward-looking statements. These risks and uncertainties include, without limitation, our ability to develop new products and evolve existing ones, customer and market acceptance of biometric solutions generally and our specific offerings, our ability to expand sales within existing customer relationships, our ability to raise additional capital, and our ability to attract and retain key personnel. For a more complete description of these and other risk factors that may affect the future performance of BIO-key International, Inc., see "Risk Factors" in the Company's Annual Report on Form 10-K for the year ended December 31, 2018 and its other filings with the Securities and Exchange Commission. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of the date made. The Company undertakes no obligation to disclose any revision to these forward-looking statements to reflect events or circumstances after the date made.

Facebook – Corporate: BIO-key International
Twitter – Corporate: @BIOkeyIntl
Twitter – Investors: @BIO_keyIR
StockTwits: @BIO_keyIR

Investor & Media Contacts
William Jones, David Collins
Catalyst Global
212-924-9800
bkyi@catalyst-ir.com