Permitium LLC Partners With Lazarus Alliance to Ensure Compliance With the FBI CJIS Security Policy

PRESS RELEASE **UPDATED: APR 5, 2017**

Permitium LLC has partnered with Lazarus Alliance to ensure compliance with the FBI CJIS Security Policy by implementing the controls in NIST Special Publication 800-53.

Scottsdale, AZ, April 5, 2017 (Newswire.com) - Lazarus Alliance, a leading provider of cyber security, governance, risk, and compliance (GRC) services, announces its partnership with Permitium LLC, which offers cloud-based software solutions that allow sheriffs and vital records offices to automate permit and records requests. Lazarus Alliance is helping Permitium develop internal cyber security controls and ensure compliance with the FBI Criminal Justice Information Services (CJIS) Security Policy.

"Permitium handles millions of sensitive records for Sheriff's and other government agencies. As such we take data security extremely seriously. In an effort to ensure that we meet the standards, we have chosen Lazarus Alliance to handle our CJIS audit. We realize that this endeavor is not a one time effort, so we look forward to our ongoing relationship with Lazarus Alliance as we continue to strive to exceed the CJIS standards" said Paul Blake, Managing Partner, Permitium LLC.

The CJIS, which was established in 1992, is the FBI's largest division. Several departments fall under its umbrella, including the National Crime Information Center (NCIC), the Integrated Automated Fingerprint Identification System (IAFIS), and the National Instant Criminal Background Check System (NICS). CJIS's databases are a centralized source of criminal justice information used by law enforcement agencies, other government organizations, corporate networks, and cloud vendors such as Permitium. Because Permitium's cloud-based software accesses CJIS's databases to perform background checks, it must comply with the FBI CJIS Security Policy.

"The FBI CJIS Security Policy isn't just a matter of data

The FBI CJIS Security Policy isn't just

security; it's a matter of public safety," explained Michael Peters, CEO of Lazarus Alliance. "If a business' database gets breached, that business and its customers can suffer tremendous losses, which is bad enough. The CJIS databases contain confidential information on ongoing criminal investigations. If they're breached, it could be a catastrophe for the entire country. The FBI CJIS Security Policy establishes a common set of user security standards to protect the integrity of these highly sensitive databases."

a matter of data security; it's a matter of public safety.

MICHAEL PETERS, CEO, LAZARUS ALLIANCE

The FBI CJIS Security Policy is over 190 pages long and covers hundreds of different security policies, procedures, and controls, including access control, identification and authentication, physical protection, incident response, and security awareness training. Commonly, organizations document security control compliance with the FBI CJIS Security Policy by "mapping" the requirements with the NIST Special Publication 800-53 framework, which uses a risk management framework to outline and document security controls for federal information systems and organizations. The CJIS publishes a document that "maps" CJIS Security Policy requirements to the applicable NIST 800-53 controls. Even with this guide, mapping CJIS standards to NIST 800-53 is a complex, exacting process that is best performed by NIST compliance experts.

"We've seen CJIS compliance reports publicly available that are totally wrong provided by other providers. We are highly experienced with NIST 800-53 and we are ISO 17020 accredited, so our work for Permitium is being done on familiar territory," Peters said. "We utilize Continuum GRC's IT Audit Machine (ITAM) software, which has pre-loaded NIST compliance modules that automate and greatly speed up the compliance process. By combining the ITAM software with our proven methodology, we have helped many organizations achieve NIST compliance on budget and on schedule."

Additionally, Lazarus Alliance is helping Permitium with the Service Organization Control 2 (SOC 2) attestation reporting process. SOC 2 reports, which utilize the AT-101 standards, are released by technology service companies to document data security controls and procedures.

"Because Permitium's software interfaces with some of the most sensitive databases in the nation, it's especially important that they release a SOC 2 attestation," Peters said. "It demonstrates to Permitium's customers that the company is committed to maintaining the highest levels of information security."

Source: Lazarus Alliance

Related **Files**

- lazarus-alliance-corporate-digital-brochure
- Continuum-GRC-Overview-2016

Additional **Links**

- Lazarus Alliance Criminal Justice Information Services (CJIS) Audit and Assessment Services
- Lazarus Alliance AT-101 SOC 2 Audit Services

Categories:

Business Technology, Compliance and Regulations, Business Security

Tags:

CJIS Security Policy, compliance, Cyber security, ITAM, NIST, SOC 2

Original Source: www.newswire.com