

Contact:
Heidi Rosenberg
Nadel Phelan, Inc.
+1-831-440-2405
heidi@nadelphelan.com

DEPARTMENT OF DEFENSE LIFTS RESTRICTIONS ON PORTABLE SECURITY DEVICES AND APPROVES IRONKEY FOR DoD USE

IronKey Exceeds Stringent DoD Requirements for Encryption, Malware Protection and Secure Supply Chain

LOS ALTOS, Calif., Feb. 19, 2010 – In direct response to the lifting of the 14-month ban on flash drives by the Department of Defense (DoD), [IronKey](#), the leader in secure and managed portable computing, today announced that it has been designated as one of the approved devices for use by Department of Defense personnel.

As one of the only Data At Rest (DAR) USB flash drive vendors, IronKey exceeds the stringent DoD requirements for USB flash media including:

- Onboard anti-virus scanning and active malware defenses
- User initiated read-only mode
- Password-protected access control
- AES 256-bit hardware encryption in CBC mode
- FIPS 140-2 Level 3 validation
- Support for McAfee Device Control Module (DCM)
- Support for CAC/PIV authentication
- Support for the Tresys File Sanitization Tool (FiST)

“Once again, we are empowered with more mobility and efficiency without compromising on security, now that premier portable devices have been approved for use within the agency,” said Craig P. Abod, president of Carahsoft. “Due to the highly sensitive nature of the information we work with, we must strictly enforce security policies to ensure that this data does not fall into the wrong hands, and is not compromised in any way. The combination of the security features, along with the remote tracking capabilities make IronKey a convenient and secure solution that allows us to enforce security policies across these devices from a centralized administrative console.”

From its inception, IronKey has worked closely with the [US Department of Homeland Security \(DHS\) Science & Technology Directorate](#) to develop next-generation crimeware defense technologies. IronKey is a trusted vendor for a number of federal agencies, including [FEMA](#), [NATO](#) and the [DHS](#). IronKey is committed to a secure supply chain, and all IronKey devices are designed and manufactured in secure facilities in the United States.

“As a security company at the core, we continuously strive to deliver the most secure mobile data solutions to our customers in the federal market,” said David Jevans, CEO at IronKey. “We have taken extensive measures to distinguish our secure drives from conventional portable storage devices, and this DoD approval is a strong validation of our efforts. We are committed to enabling flexibility and mobility, while ensuring that confidential information remains secure, and that government networks are protected.”

Unlike conventional USB flash drives and memory sticks, IronKey government-approved devices provide intelligent secure storage with military-grade [hardware encryption](#), strong, two-factor [authentication](#) and on-board security features. IronKey integrates [best-of-breed anti-malware](#) scanning technology to prevent [malware](#) from infecting IronKey secure storage devices, and then spreading onto networks. IronKey includes the ability to disable the [AutoRun](#) capabilities of Microsoft Windows, which can be exploited to infect computers when a compromised USB drive is plugged in.

IronKey devices support one-time password technology including [RSA SecurID®](#), allowing IronKey to be used as a two-factor token, and eliminating the need for federal workers to carry multiple devices. IronKey USB drives can be centrally [managed remotely](#), allowing administrators to track device use, provide automated security and anti-malware updates, and even remotely disable devices in case of loss. With IronKey, organizations can create a trusted access network, with restrictions in place that prevent the drives from mounting on untrusted host systems. IronKey devices have been [validated](#) to meet the rigorous government security requirements of [FIPS 140-2 Level 3](#), ensuring that its housing is both tamper-proof and tamper-evident.

About IronKey:

IronKey is the global leader in providing secure and managed portable storage, authentication, and trusted virtual computing solutions for mobile workers. IronKey multifunction portable security devices, management software and associated services are designed to meet the security, performance, and privacy standards of the most demanding enterprise and government customers. IronKey solutions range from IronKey Basic, the world’s most secure USB flash drive, to the IronKey Enterprise Virtual Desktop solution for carrying a secure operating system and virtual desktop environment on a pocket-sized device. IronKey works with industry leaders in virtualization, storage and security, including Lockheed Martin, McAfee, MokaFive, RSA, RingCube and VeriSign to extend the applications of its secure mobile computing platform. IronKey products are FIPS 140-2, Level 3 validated. Thousands of customers use IronKey, including Fortune 500 companies, enterprise organizations in financial services, healthcare and legal markets, as well as government agencies, including FEMA, NATO and DHS. For more information, please visit www.IronKey.com.