FAQs on CJIS Advanced Authentication

This seeks to answer the questions, clarify some misunderstandings, and communicate some changes to the CJIS Security Policy 5.1 requirements for Advanced Authentication (AA). Agencies must immediately implement AA technology if Criminal Justice Information (CJI) is transmitted or received on a computer device located outside of a secure location. A clause in the CJIS Security Policy 5.1 allows for a police squad car to be considered a physically secure location, if the computer devices were purchased before 2005. Additionally, IPSec (a protocol suite for securing Internet protocol communications) could be used as a way to meet the AA requirements, if IPSec was implemented or funds to implement were acquired prior to February 2011. In either case, the exception clauses were scheduled to sunset on a deadline of September 30, 2013, and January 30, 2013 respectively. However, the CJIS APB recently voted to delay the sunset deadline to September 30, 2014. This change was made official by the APB on February 20, 2013.

FAQ's

Question - What is Advanced Authentication (AA)?

Answer - Advanced Authentication (AA) refers to a security approach supported by technology and software to better ensure the identity of an individual. Most systems require a User ID (UID) and password. However, the sensitivity of information and systems connected to the FBI/CJIS warrant an additional authentication step when the device used for access is outside a secure location. AA is sometimes referred to as "Two-Factor" Authentication, which gives a clue as to what constitutes AA. AA would comprise at least two of the following factors: 1) Something you know; 2) Something you are; and 3) Something you have. Something you know would be a password or PIN. Something you are would be a fingerprint, retina scan or hand geometry. And, something you have could be a grid cipher or a PIN generator usually from a fob device. The AA solution accepts the collection of this type of information and upon a successful challenge opens the device to the individual.

Question - Do the AA requirements apply to my agency?

Answer - Yes, the AA requirements apply to all criminal justice agencies transmitting or receiving CJI outside of a physically secure location.

Question - Can I wait until September 30, 2014 to implement AA?

Answer - If you have computer devices located in a physically non-secure location where the user accesses CJI and those devices were purchased after 2005, the answer is no. You are required to immediately implement AA because your devices were purchased after 2005.

Question - Our agency's officers access CJI in their squad cars, through a mobile network on Mobile Data Computers (MDC) that were purchased in 2004. Do I need to immediately acquire and implement AA?

Answer - AA can be an expensive and complicated solution, so your agency should begin immediately to find an AA solution. However, since your computing devices were purchased prior to 2005, your agency's squad cars are considered a secure location based on the exception clause located in CJIS Security Policy 5.1. However, that exception clause will sunset on the September 30, 2014 deadline.

Question - Our agency implemented IPSec in December of 2010 to meet the AA requirement. Is our agency compliant or do we have to implement some other solution?

Answer - Because your agency implemented IPSec prior to February of 2011, the IPSec solution is compliant until September 30, 2014. However, after September 30, 2014, IPSec will no longer qualify as an acceptable AA solution. Your agency will need to acquire and implement an AA solution.

Question - What AA solution does the Illinois State Police endorse or recommend?

Answer - There are a number of qualified vendors and solutions in the marketplace. The ISP cannot recommend or endorse any solution or vendor. Your agency's Information Technology (IT) Department or IT contractor should provide recommendations that are tailored to your agency's IT requirements.