HSPD-12 and FIPS 201 – How Are They Related?

For Government, Say "FIPS!"

By April Dalton-Noblitt, Ingersoll Rand Security Technologies
For Government Sales, Say "FIPS!"

It's important to note that state and local codes apply to all state, county and municipal government security purchases and installations, both public and private. It is also important for non-federal government entities to know what other codes must be met in addition. In some cases, federal regulations may be replicated as well.

Two Primary Programs Apply…HSPD-12 and FIPS 201…But They're Related!

Homeland Security Presidential Directive 12 (HSPD-12) is fueling smart card use in the government and accelerating adoption by large enterprises. HSPD-12 seeks to establish secure and reliable identification for all federal employees and contractors.

Federal mandates tend to have a cascading effect, so this directive ultimately has huge significance because state and local governments, as well as first responders, will need to convert to FIPS 201-compliant smart cards in order to follow the federal initiatives. Private contractors must follow and are doing so, including Boeing and others.

To meet the requirements of HSPD-12, the National Institute of Standards and Technology (NIST) published a standard for secure and reliable forms of identification, Federal Information Processing Standard (FIPS) 201. The FIPS 201 Personal Identity Verification (PIV) card standard requires contact and contactless smart card technologies and biometrics and provides specific standards for the issuance and use of the PIV card.

The key thing to remember is that FIPS 201 sets specific technology standards but does not specify the physical access control system. The card and biometric standards addressed in FIPS 201 deal solely with the technologies used in authenticating individuals at the credentialing offices or visitor centers so that credentials produced

work on a wide variety of readers. The federal requirements do not, at this time, address the physical access control system.

Here is what you need to do: Verify that your reader technology meets the PIV card interoperability standards and that the physical access system will communicate with that reader.

A qualified card and reader manufacturer can help you do so and will help you specify FIPS 201 compliant readers.

Where You Can Get into Trouble

A mixed population of old proximity credentials and new PIV II credentials often will be unavoidable when pursuing an upgrade path to FIPS 201 compliance. And most are not thrilled with having to install two different types of readers to accommodate a transition. If this scenario applies to your migration, select multi-technology readers which are compatible with both FIPS 201 PIV II credentials and popular proximity and smart card technologies.

Reading multiple existing card types and PIV II cards simultaneously is a tremendous benefit to anyone looking to painlessly transition.

You can't afford to purchase security solutions in a legislative vacuum. Being aware of federal standards and regulations that affect both government and non-government entities alike will help you to choose a qualified vendor, and appropriate security solutions that will meet your needs today and into the future while keeping you in compliance with the latest laws and regulations that affect the industry.