



## The evolution of identity

At its most fundamental, security continues to encompass the ability to identify the individuals entering your facilities, accessing your physical property and leveraging your logical assets. But as identity theft and cyber attacks become more pervasive in our society, security strategies must evolve to a new level of sophistication. Modern tools must enable agencies not only to verify a persons identity, but also to manage their access to property and information assets. Simply requiring the presentation of an identification card at a facility's entrance is no longer enough.

*In today's environment of border patrols, no-fly lists, chemicals of interest and color-coded threat levels, security is more important than ever before. That's why government agencies are taking unprecedented steps toward a holistic security strategy that will ensure the protection of the homeland today and in the future. Diebold Security can help.*

The 12<sup>th</sup> Homeland Security Presidential Directive (HSPD-12) provides government agencies with a defined policy for establishing the identity of employees and contractors, as well as for the creation of a secure credential. That policy resulted in a credentialing process, defined by Federal Information Processing Standard (FIPS) 201 and supported by the associated NIST Special Publications requiring a uniform approach to the creation and issuance of a common identification credential. These credentialing standards are encompassed by and work in conjunction with the FIPS 201 PIV standard. This approach, which is intended to enable interoperability from agency to agency, includes vetting, verification and authentication of identity in order to grant access to federally-controlled facilities and information systems.

The implementation of this new approach to security is no small task. And it requires an unprecedented level of cooperation among agencies' human resources, information technology and security departments. Government agencies must understand the requirements: coordinate disparate legacy systems; enhance those systems with new, network-driven tools; and enroll thousands of people in the program. And with a security partner like Diebold, it doesn't need to stop there. You can leverage your investment in these secure identity credentials to include access management, as well as the provisioning of identity information for consistent use by multiple systems throughout your enterprise. Such a long-term approach to identification and access management will help ensure the value and sustainability of your security strategy – across multiple agencies and locations – for years to come.