



**2008-2**

## **NATIONAL SHERIFFS' ASSOCIATION ADOPTS FEDERAL INFORMATION PROCESSING STANDARD**

WHEREAS, the Office of Sheriff is the highest constitutional law enforcement office in counties throughout the Nation and, as such, Sheriffs occupy near-ubiquitous positions of authority and responsibility for law enforcement, public safety and front-line homeland security for the Nation;

WHEREAS, in response to Homeland Security Presidential Directive 12, and in order to better protect Federal facilities from 21st century threats, the Federal Government has adopted the Federal Information Processing Standard 201 ("FIPS 201") standard promulgated by the National Institute for Standards and Technology ("NIST") as its vehicle for authenticating the identities and credentials of Federal employees and contractors needing access to Federal facilities, and Federal agencies have begun the process of implementing millions of FIPS 201 "smart cards" as a means of better securing Federal facilities;

WHEREAS, in order to better prepare the Nation to respond to law enforcement, public safety, and homeland security threats and incidents, Federal state and municipal governments around the Nation have begun various initiatives to encourage or require the issuance and use of FIPS 201-based identity authentication credentials by first responders and by public and private sector persons needing to enter secure non-Federal facilities and reenter local disaster areas;

WHEREAS, the FIPS 201 standard issued by NIST is an evolving general standard which may be implemented by card and equipment vendors in a variety of ways, such that, unless prompt action is taken, Sheriffs and other local law enforcement perimeter control gatekeepers will be put in the position of dealing with a large variety of FIPS 201-based credentials which are not interoperable and which utilize a variety of resource typing and other data formats incompatible with national standards recognized by perimeter control gatekeepers;

WHEREAS, Sheriffs and their law enforcement partners, nationwide, undertake the nation's first and primary responsibility for manning the nation's perimeter control checkpoints and, as such, are determined to avoid interoperability and compatibility problems which will inevitably arise when presented at such checkpoints with non-standard FIPS 201-based credentials;

WHEREAS, the NSA Standards & Ethics, Education & Training Committee (the "Committee") has

recommended that the Executive Board of NSA adopt the FIPS 201 Standard approved by the Committee, together with such revisions thereto as may be subsequently approved by the Committee (the “NSA FIPS 201 Standard”);

WHEREAS, the NSA FIPS 201 Standard contemplates a close working relationship between Sheriffs and card vendors in enrolling, conducting background checks to vet, and issuing First Responder Authentication Credentials “FRACs”), disaster reentry credentials and other FIPS 201-based credentials for persons other than Federal personnel and facilities; and

WHEREAS, the Pegasus Program is prepared to certify, within the policy guidance of the Pegasus Advisory Board of the NSA, one or more vendors of FIPS 201-based credentials as compliant with the NSA FIPS 201 Standard.

NOW, THEREFORE, BE IT RESOLVED, that:

1. The NSA FIPS 201 Standard is hereby adopted by the National Sheriffs’ Association for implementation and recognition by Sheriff’s Offices and their law enforcement, public safety and homeland security partners nationwide;
2. The National Sheriffs’ Association recognizes the Pegasus Program as its Certification Authority to certify compliance with the NSA FIPS 201 Standard; and The National Sheriffs’ Association calls upon the Department of Homeland Security to include the reasonable vetting, issuance, and maintenance and training costs of NSA FIPS 201 Standard-compliant FRACs as allowable equipment and training costs for purposes of UASI, CEDAP and other similar DHS equipment and training programs.