

1. [What is the Tiers of Trust Program?](#)
2. [Who is eligible for the Tiers of Trust Program?](#)
3. [Why is the Trusted Tiers Program being made available for First Responders?](#)
4. [Why do we need First Responder Access Credentials \(FRAC\)?](#)
5. [What about the Trust Model for Issuance and Ongoing Administration?](#)
6. [How Does the Trusted Tiers Program Work?](#)
7. [What About the Technology of the Smart Cards?](#)

- **What is the Tiers of Trust Program?**

For secure and reliable forms of identification, HSPD-12 states that “The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security...” The Tiers of Trust program implements this risk-based concept, initially for First Responders, as well as NIMS for credentialing and resource typing. While most emergency situations are handled locally, when a major incident occurs skilled resources may be deployed to/from neighboring jurisdictions, in addition to state and federal response officials. Not every first responder may be deployed to a national event, yet they need a less-costly, high-security smart card credential for identity and skills verification that is interoperable and FIPS 201 compliant. Just as privilege levels differ across roles and levels, the majority of a jurisdiction’s response teams can now utilize a more cost-effective, locally-controlled solution versus expensive ‘one size fits all’ dual interface cards. The resulting credentials are also multipurpose, providing high assurance of identity for daily building access as well as id/skills verification in the field.

The Tiers of Trust program enables a locally-controlled FRAC (First Responder Access Credential) system using the same contactless interface as expensive dual interface cards. Tiers of Trust partners are offering substantially-discounted packages for creation/usage of contactless credentials. For verified First Responder organizations, the SNS Write-IMPACT™ software is being offered at no charge. Write-IMPACT has an easy-to-use interface for programming mandatory FIPS 201 data for contactless smart cards. Add-on modules increase the capabilities including applying strong encryption to the contents.

Featuring the new Emergency Management One™ DESfire card stock, credentials are more durable in adverse conditions. These cards were specifically engineered and built for this purpose by HID Global. Thirty-one of the Tiers of Trust package components are [US GSA certified for FIPS 201](#), and SNS is SIN 132.62 [GSA certified as a Qualified HSPD-12 Service Provider](#) for a Complete end-to-end solution. The [Tiers of Trust](#) program supports all of the FIPS 201 requirements and guidelines for issuance and ongoing usage and NIMS for credentialing and resource typing.

- **Who is eligible for the Tiers of Trust Program?**

Legitimate First Responder organizations within the United States of America and US territories are eligible. This includes law enforcement, fire, hazmat, rescue, and public health organizations as well as private sector utilities, communications, and transportation companies. Applications are due by 12/31/2007 with priority to the first 500 organizations.

The program embraces large through small organizations; however the highest ranking official within the organization must acknowledge and approve participation in the program. Appropriate management commitment is a requirement to ensure the predetermined level of trust is established, accredited officially, and maintained.

Tiers of Trust FAQ

- **Why is the Trusted Tiers Program being made available for First Responders?**

SNS and our partners share a deep commitment to ensuring our nation's First Responders have access to affordable, high-quality offerings for trusted identity credentials that are FIPS 201 compliant and interoperable. These inexpensive yet technologically impressive packages can equip a jurisdiction to issue authorized first responder smart card credentials for identity and training certification verification, and to use them in both daily facility access and at emergency field sites. As a tribute to the importance of our nation's first responders, the Trusted Tiers partners are dedicated to providing reliable, rapidly-verified solutions that meet or exceed the security standards at a fraction of the cost of alternative dual interface cards.

Tiers of Trust partners believe our nation's first responders deserve the highest security for their own identities, as well as their own safety while in controlled areas. Smart card based photo identification credentials are significantly more secure than plain PVC cards due to proven resistance to cloning, counterfeiting or forgery. Thus as a foundation, smart card based cards are key for protection of personal identity information and allow unsurpassed assurance compared to insecure, scrambled bar codes or other legacy technologies. Also the ability to achieve effective access control by assurance of authenticity with a high degree of confidence is enhanced by orders of magnitude. However, dual interface cards are expensive initially and annually. Leveraging the contactless Emergency Management One™ card stock is substantially less costly and more durable than dual interface cards with a gold contact chip, and the ability to control access to areas is absolutely equivalent and FIPS 201 compliant. We support America's First Responders!

- **Why do we need First Responder Access Credentials (FRAC)?**

During the 9/11 attacks we lost over 300 first responders in NY and could not account for each of them, and necessary response officials rushing to the Pentagon were denied entry because an interoperable system was not in place. During the Hurricane Katrina recovery, licensed medical personnel could not prove their skills and certifications and thus were not deployed effectively. Even smaller jurisdictions with low turnover may require the ability to possess valid FRAC credentials if a situation escalates to multi-agency. These common sense reasons are echoed by HSPD-5, HSPD-8 and HSPD-12 regulations as well as the National Incident Management System (NIMS).

National Incident Management System (NIMS) Compliance

In order to receive federal preparedness grant funds, certain goal dates have been established for National Incident Management System (NIMS) compliance. For fiscal year 2007, interoperable credentialing and resource typing of response assets conformance are being [measured](#). Published by the Department of Homeland Security in 2004, NIMS was mandated by Homeland Security Presidential Directive (HSPD) -Management of Domestic Incidents and [HSPD-8](#) Preparedness. [HSPD-5](#) dictated that Federal departments and agencies adopt NIMS as a requirement for the provision of Federal preparedness assistance funds. Overall, NIMS was developed so responders from different jurisdictions and disciplines can work together better to respond to natural disasters and emergencies, including acts of terrorism.

[NIMS](#) provides a comprehensive and consistent national approach to all-hazard incident management at all jurisdictional levels and across all functional emergency management disciplines. Augmented by the NIMS Integration Center within DHS, the DHS Science and Technology Directorate and the National Institute for Standards and Technology (NIST) are establishing working groups to [extend the FIPS-201 smart card standard](#) to address first responder credentials and to ensure the various implementations will be interoperable nationally. The Tiers of Trust program supports all of the NIMS credentialing and resource typing requirements/guidelines for issuance and ongoing usage.

HSPD-12 Compliance and FIPS 201

Tiers of Trust FAQ

Federal employees and contractors accessing secure Federal and other facilities (computing resources and buildings) are required to possess secure and reliable forms of identification per [HSPD-12](#). The standard includes graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security. Thus the HSPD-12 directive itself calls for Tiers of Trust.

Federal Information Processing Standard (FIPS) 201, entitled *Personal Identity Verification of Federal Employees and Contractors*, was developed to satisfy the requirements of HSPD 12, approved by the Secretary of Commerce, and issued in 2005. In addition, a number of guidelines, reference implementations, and conformance tests have been rolled out, and thirty-one of the current Tiers of Trust package components are [US GSA certified for FIPS 201](#), and SNS is SIN 132-62 [GSA certified as a Qualified HSPD-12 Service Provider](#) for a Complete end-to-end solution. The [Tiers of Trust](#) program supports all of the FIPS 201 requirements and guidelines for issuance and ongoing usage.

- **What about the Trust Model for Issuance and Ongoing Administration?**

The HSPD-12 mandate specifies that issuing providers must have their reliability established by an official accreditation process. Organizational policy and procedures for issuance are critical to establishing and maintaining a pre-determined level of trust as the credentials are issued utilized within and between organizations. Tight control of card stock, background check processes, and strictly limited access to printing (graphical personalization) and programming (electronic personalization) facilities are essential. Rigorous ongoing administration of the credential database, for example additions, modifications, and terminations is important to have in place, and also serves to protect sensitive identity records.

Tiers of Trust is offering affordable web-based training courses and certification exams for issuance and administration, and jurisdictions are highly encouraged to take advantage of certifying their systems as another degree of assurance to reinforce the trust level chosen.

- **How Does the Trusted Tiers Program Work?**

Interested First Responder organizations may submit a completed Registration Form for verification, and receive acceptance into the program in as little as 24 hours. Once approved, the organization may place orders for Minimum and Optional Components at special pricing. The SNS Write-IMPACT™ software program is being offered at no-charge for CHUID/FASC-N and expiration date writing and reading (feature code 1001), and special contactless smart card stock and US GSA FIPS 201 approved reader/writer units are bundled into packages that can be tailored to meet an organization's specific requirements.

Tiers of Trust FAQ

- **What About the Technology of the Smart Cards?**

Dual interface cards have a contact chip and a contactless chip and antenna. These full PIV cards are well-suited to computer logon, but suffer in Emergency Management environments where the gold contact chip can be damaged by chemicals, salt water, decontamination washes, and particulated air like soot and smoke. They are very expensive, and are only offered through approved managed services providers. They can be utilized by the SNS NIMS-IMPACT® and CRITSEC® systems for access control to zones at an incident or to secured buildings or rooms because of their FIPS 201 mandated contactless interface.

Traditional contactless chip/antenna cards are 125 kHz proximity or Prox and do not have any storage, while the newer 13.56 MHz DESfire contactless chips/antenna cards have storage capacity for personally-identifying information. Contactless data transfer is much faster. Card stock with both contactless chips over the different frequencies are available, and can ease the transition to HSPD-12 compliance. However quality of signals and non-interference of poorly-manufactured cards is a concern, as these are not quite commodity items today.

DESfire V6 cards have 4K of storage, and future DESfire V8 cards double that storage to 8K capacity. As the capacity expands, the ability to store larger encrypted data files, like fingerprint templates and color digital photos will be made available. The information stored on the contactless chip can be encrypted using the FIPS 140-2 Triple DES (or 3DES) algorithm, which is US NIST certified for strong encryption. HID Global has engineered and built the Emergency Management One™ DESfire V6 cards using composite materials (60% PVC, 40% PET) for strength and durability especially for the Tiers of Trust program. These cards also carry HID's lifetime warranty.

Please see the diagram below for more information on storage capacities and attributes:

