SUMMARY PAGE

Public Meeting on Proposed Identification Standard for Federal Employees and Contractors

On January 19, 2005, a public meeting is scheduled to discuss the policy, privacy, and security issues associated with Homeland Security Presidential Directive-12 "Common Identification Standard for Federal Employees and Contractors." Karen Evans, Administrator for E-Government and Information Technology is the keynote speaker. Ms. Evans will be followed by 2 panels to discuss key policy questions.

Due to the number of responses from individuals interested in attending this meeting, there will be a second meeting in the afternoon at the same location. The afternoon session will be held at the same location, from 1–4pm and will cover the same topics.

Because of space limitations, attendees may only attend one session. Due to resource constraints, Attendees registered for the morning session, may not switch sessions.

Location: Auditorium of the Potomac Center Plaza, 550 12th Street, SW, Washington, DC, near the Smithsonian and L'Enfant Plaza Metro Stations.

Registration Information:
The meeting is open to the public and there is no fee for attendance. All attendees must pre-register and present government-issued photo identification to enter the building. To attend, your registration information must be received by 5 pm, EST, January 11th. No late registrations will be accepted. Please send your name and affiliation to: Sara Caswell, NIST, Sara.caswell@nist.gov.

Additional information will be posted here. The agenda and list of speakers will be posted on January 10th.

Meeting Discussion Topics

Speakers are asked to discuss key questions, such as:

1. How do the proposed technologies in the draft FIPS 201 standard affect privacy and security?

    - Does the proposed use of contact and contactless smart card chips raise privacy or security concerns?
    - Do the biometric (fingerprint and facial image) standards, as proposed, raise privacy or security concerns?
    - Does the assignment of a permanent or persistent employee identification number raise privacy concerns?
    - Do other applications or features of the card, as propose raise concerns?

2. Do the proposed credential issuance policies and procedures raise privacy and security concerns?

3. What federal uses of the identification raise privacy and security concerns?

4. Are there means to address privacy and security in the development of the card standard and implementation guidance?
   - Can privacy enhancing technologies be built into the card?
   - How can we limit non-federal uses of the card?
   - What training do employees and contractors need to properly use secure their cards?
   - What training should card issuers have? Security personnel?
   - What law and policies must agencies consider in planning for and implementing the new cards?

AGENDA

The agenda will be posted here on January 10th.