COMMON IDENTIFICATION STANDARD
Potamac Center Plaza
550 12th Street, SW
Washington, DC 20004
10th Floor Auditorium

Remarks by Gary E. Clayton
Jefferson Data Strategies, LLC

Thank you for the opportunity to provide comments today regarding the Federal Personal Identity Verification (PIV) Standard issued by NIST and the Department of Commerce. My name is Gary Clayton and I am the CEO of Jefferson Data Strategies (Privacy Council). We have been actively involved in the development of effective management processes and tools to ensure the protection of privacy. We work with both governmental agencies and private industry. We are currently managing the overall privacy program for the Department of Transportation and are involved in a number of initiatives related to Homeland Security programs. These experiences have given us a unique perspective on effective privacy management in technology programs.

I appreciate the need for a single standard for identity cards for employees and contractors. The current system makes it hard to achieve the goals of efficiency and of security for the cards and the personal information associated with them. The proposed standard appears to have the flexibility to support a wide variety of services and uses, while still providing a standard look and information set.

What appears to be missing from the standard, however, are significant input and/or specifications for an adequate policy framework to prevent misuse of the cards themselves and of the associated data. Those involved in the development of the proposed standard appear to have made a mistake common to most technology projects: the technology has been designed without adequate involvement and input on privacy and policy. The review of the proposed standard and the comments received to date seem to indicate that the standard has been developed before understanding and/or adopting the necessary policies to protect privacy. Indeed, the failure to adopt such policies before specifying the technologies and their design puts at risk both the privacy and security of cardholders and the systems involved. You are to be congratulated, however, for the opportunity to present and discuss the policy and privacy issues surrounding the proposed standard.

The current draft does not appear to contemplate a comprehensive privacy strategy that serves as the foundation from which the PIV Standard is to be built. It has been our experience in working with governmental agencies and commercial entities that fidelity to widen accepted privacy principles and processes will serve as effective risk management tools – and will increase both security and privacy. The Fair Information Practices are fundamental principles that should be addressed as appropriately in the standard. There should be clearly defined standards to limit the condition under which agencies may acquire, access, store and use personal data and biometric data.

As discussed below, the failure to address the application of such principles will increase the risks to privacy and security.

1. **Mission Creep:** the standard contains no guidance or controls on mission creep. There are two aspects to this: First, the broad description of possible uses makes it almost inevitable that there will be broader and broader use of the PIV Cards and technology to many additional areas. Second, the FIPS states that position sensitivity levels are to be determined by departments and agencies. The absence of a system wide policy on position sensitivity levels not only creates security issues, but also gives card issuers enormous discretion regarding the conduct of background checks and personal information gathering. I am concerned that the tendency will be for agencies to collect the highest level of data for almost every use – unless guidelines are established.

2. **Data Retention and Standard Uses:** there is little information on intended use and data retention. The public draft should include details about which routine uses of personal data, how long the data will be kept, what system of records the data enters, where or how copies are to be kept and what sort of protections and privacy policy should be in place regarding such data.

3. **Source Documents:** the applicants are required to provide “two forms of identification from the list of acceptable documents included in the Form 1-9. The standard contemplates that these documents are to be photocopied and sent to the sponsoring organization. These documents can include copies of

SSN cards, drivers' licenses and other highly sensitive documents. You should consider putting in place detailed access, use and privacy policies before any such information is collected. The standard should also address the retention of such documents.

4. **Section 2.3: Identity Credential Issuance:** Under Section 2.3, the Issuing Authority shall be responsible to maintain: complete and formally authorized PIV Request; the name of the PIV identity credential holder; the credential identifier such as an identity credential serial number; and the expiration date of the identity credential. Section 2.3 does not, however, contain any controls for limiting the use of the "credential identifier." Appropriate uses should be discussed and included in the official framework.

5. **Registration Database:** Section 5.1.1: the standard does not specifically discuss the process by which individual access to the database will be controlled. Because of the sensitivity of the data, it is important for there to be common standards across the government.

6. **Limitations in the Amount of Data Obtained:** authentication requirements should be set depending on the sensitivity of the transaction involved. Requirements should be set depending on the sensitivity of the transaction. The authentication required for any class of transactions should be no stronger than is necessary for the specific purpose. The standard should specify that specific programs or transactions get only the information needed at the time that they need it for the level of sensitivity involved.

7. **Contact versus Contactless Cards:** the technologies involved in the two types of cards appear to reasonably address the security issues associated with contactless cards. One of the issues regarding contactless cards is the ability to read the cards without the owner's knowledge. The risks associated with this appear to have been adequately addressed by the proposed standards. A privacy issue should be considered, however. It is my understanding that a contactless card offers greater storage capacity for data. With greater capacity, the tendency is going to be to use the space to capture

more and more information about the owner. Guidelines should set controls on the type and amount of data that can reasonably be captured and stored.

8. **Biometric:** the concerns about privacy related to the use of such biometric information appear to be primarily related to the security of such information. These concerns appear to have been addressed.

9. **Permanent or Persistent Employee ID Concerns:** as noted above, the uses of such unique identifiers should be detailed and controls put in place. The tendency is going to be to use such unique identifiers for more and more purposes – unrelated to those contemplated currently. The standards should include policy, controls, and guidelines on the appropriate use and deletion of the permanent or persistent employee ID.

Issuance of Draft Policies on Privacy: Prior to the issuance of the final standard, we believe that it is imperative to issue draft policies for public comment. A common mistake by technologists is to design the technology and then involve policy and privacy as an afterthought. As a result, policy issues are not addressed nor resolved. Technologies fail to garner public support and/or trust. This should be avoided for this important initiative. NIST should seek the involvement of the public and OMB with the standards and seek additional comment and input on privacy and policies. Failure to undertake this essential step can put the technology at risk.