

X-Sieve: CMU Sieve 2.2
Date: Thu, 23 Dec 2004 11:06:59 -0600
From: Larry Price <lprice@anl.gov>
X-Mailer: Mozilla 4.79 [en] (Windows NT 5.0; U)
X-Accept-Language: en
To: DraftFips201@nist.gov
Subject: Comments on Public Draft FIPS 201
X-MailScanner:
X-MailScanner-From: lprice@anl.gov

December 23, 2004

To: FIPS201 NIST
From: L. E. Price Chairman, ESnet Steering Committee
Subject: Concerns about FIPS PUB 201 Draft

I am writing as the chairman of the ESnet Steering Committee (ESSC). ESSC is a committee of scientific users and managers of ESnet, which is the national computer network that provides high performance data communications to support programs in the Department of Energy (DOE), especially those of the Office of Science (OSC). Since OSC programs and science in general is done in a highly international way, ESnet supports connections to research and education networks in many other countries and regions. The network, in turn, provides access to computing and other facilities in U.S. National Laboratories and some universities to government and contractor employees and non-government participants in government-sponsored scientific programs and facilities. Connections to foreign networks provide, in a reciprocal way, access to U.S. facilities for foreign scientific collaborators and access to facilities of foreign collaborators for U.S. collaborating researchers.

The first area of concern is about the extensive and central need that exists in scientific facilities of the DOE, including those accessed by ESnet, for routine and repeated access by users and participants who are not employees of the government or of government contractors. In the Abstract, page v, the Applicability is described as "This standard is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information systems." The standard seems to

imply that it is only needed to provide a means of access for government employees and contractors to Federally-controlled facilities and proceeds to describe a particular plan for controlling that access.

However, access by users, scientific collaborators, and other participants in DOE science programs who are not government employees and contractors is a crucial and central part of these programs. These people needing access will be employed at U.S. and foreign universities and other institutions and will have (in both instances) U.S. and foreign citizenship. If there is no provision for access by these people and, as a result, access is denied or made unreasonably difficult or cumbersome, the objectives of most DOE science projects will be disrupted and compromised.

The specific access methods proposed in the document, consisting of a high tech card with multiple means of authentication, is presumably not extensible to this broad community of users and scientific collaborators. The government would probably not want to extend this form of ID to a broader class of users and, on the other side, the process of obtaining the IDs would be unreasonably cumbersome for university and foreign users and would effectively prevent their use.

Since broader access to DOE user facilities is central to the scientific mission of the agency and since the proposed access method will not be extensible to this broader community, there should be a provision for a class of federal facility for which less restrictive access is provided. Access to user facilities which are by their nature used collaboratively should continue to be under the control of the laboratory or institution that operates the facility without unworkably onerous procedures.



[NIST PIV Comments.doc](#)


ARGONNE NATIONAL LABORATORY

9700 S. Cass Avenue, Argonne, IL 60439

FAX: (630) 252-5047

INTERNET: lprice@anl.gov
630-252-6295

December 23, 2004

To: FIPS201 NIST
From: L. E. Price  Chairman, ESnet Steering Committee
Subject: **Concerns about FIPS PUB 201 Draft**

I am writing as the chairman of the ESnet Steering Committee (ESSC). ESSC is a committee of scientific users and managers of ESnet, which is the national computer network that provides high performance data communications to support programs in the Department of Energy DOE), especially those of the Office of Science (OSC). Since OSC programs and science in general is done in a highly international way, ESnet supports connections to research and education networks in many other countries and regions. The network, in turn, provides access to computing and other facilities in U.S. National Laboratories and some universities to government and contractor employees and non-government participants in government-sponsored scientific programs and facilities. Connections to foreign networks provide, in a reciprocal way, access to U.S. facilities for foreign scientific collaborators and access to facilities of foreign collaborators for U.S. collaborating researchers.

The first area of concern is about the extensive and central need that exists in scientific facilities of the DOE, including those accessed by ESnet, for routine and repeated access by users and participants who are not employees of the government or of government contractors. In the Abstract, page v, the Applicability is described as "This standard is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information systems." The standard seems to imply that it is only needed to provide a means of access for government employees and contractors to Federally-controlled facilities and proceeds to describe a particular plan for controlling that access.

However, access by users, scientific collaborators, and other participants in DOE science programs who are not government employees and contractors is a crucial and central part of these programs. These people needing access will be employed at U.S. and foreign universities and other institutions and will have (in both instances) U.S. and foreign citizenship. If there is no provision for access by these people and, as a result, access is denied or made unreasonably difficult or cumbersome, the objectives of most DOE science projects will be disrupted and compromised.

The specific access methods proposed in the document, consisting of a high tech card with multiple means of authentication, is presumably not extensible to this broad community of users and scientific collaborators. The government would probably not want to extend this form of ID to a broader class of users

and, on the other side, the process of obtaining the IDs would be unreasonably cumbersome for university and foreign users and would effectively prevent their use.

Since broader access to DOE user facilities is central to the scientific mission of the agency and since the proposed access method will not be extensible to this broader community, there should be a provision for a class of federal facility for which less restrictive access is provided. Access to user facilities which are by their nature used collaboratively should continue to be under the control of the laboratory or institution that operates the facility without unworkably onerous procedures.

LEP:sak