Subject: US Department of Justice Comments on Draft Department and Agency Implementation Guidance Homeland Security Presidential Directive 12

Re: (a) Draft of Subject Document, issued by Karen S. Evans on 4/1/05

From: Department of Justice

Thank you for the opportunity to provide comments. We have the following questions/comments regarding the plan, and ask that you consider them before issuing the final version of the document:

Issues of Primary Concern:

1) **The prescribed process for obtaining NAC clearances will cause significant mission critical harm by unnecessarily delaying key personnel and contractors "start dates" due to the length of time required for follow-up on exception conditions associated with the "FBI Name Check" process.**

   Although the quoted "service level" for NAC processing is two to five days many take significantly longer and there is not a streamlined exception process**.** However, the NAC component that requires the most time to complete is the FBI name check, and the FBI identifies that their current processing time for name checks is as follows:

   - Number received each month 80,000
   - Number completed in 72 hours 60,000 (75%)
   - Number completed in 60 days 68,000 (85%)
   - Number completed in 120 days 78,800 (96%)
   - Number completed in 365 days ~80,000 (~100%)

   Therefore, 15% of the time, the name check component of the NAC will take longer than 60 days, and this assumes the current processing volumes, not the volume to be expected as all Departments and Agencies seek to comply with FIPS 201. The law enforcement mission is vital and the current processes that will be terminated allowed for a workable and controlled exception process by DOJ so as not to negatively harm important operations. In addition, the prescribed process does not take into account the special situations, such as a change in administration, where there is an abnormal peak in NAC processing volumes for sensitive and mission critical positions that must be quickly accommodated in order to smoothly carry out the federal law enforcement mission.

2) **The identified date for FIPS 201, Part 2 compliance of 10/27/06 is too aggressive.**

   A significant number of items regarding HSPD-12 are still unresolved, and impact an implementation of the Directive: They include:

- All of the final technical specifications for implementing Part 2 of FIPS 201 have not yet been released, including Special Publication 800-76.
- Private sector hardware and software companies do not currently have the ability to comply with Part 2 of FIPS 201, nor have they gone through the required certification and accreditation process.

- Testing of minutiae processing for fingerprint verification will not be completed until February 2006 and there is not a workable CONOPS for the authentication of fingerprints for physical access to facilities or logical access to systems. Without a workable CONOPS DOJ will not be able to implement this security feature of the directive.

- GSA contracts are not yet in place for the procurement of required components and services, nor has the GSA developed a CONOPS for interoperability between different Departments and Agencies that are in shared environments.

- A CONOP for the protection of personal privacy in a contact-less smart card environment needs to be produced.

- Department of Commerce will not issue the reference implementation document to aid Department or Agency implementation until 6/25/05 which is too late to utilize during the formulation of the mandatory Agency Plan due 6/27/05.

- OMB has yet to issue the Final version of FIPS 201 Implementation Plan guidance that is to be used to satisfy the 6/27/05 compliance date for implementation plan submission by the Department or Agency.

- Compliance with FIPS 201 as an un-funded mandate will require a Department-wide re-budgeting effort

Once all of the above have been addressed, the Department will still need significant time to identify which facilities and systems need to comply with HSPD-12 and which should be exempt, and to create an implementation plan, procure components, pilot the systems, and then rollout the initiative across the Department. Until then, the number of assumptions required to formulate a logical plan for its implementation will likely make it an impractical plan to carry out.

While DOJ understands that a firm date for compliance with FIPS 201, Part 2 is necessary, we believe that it should allow the Department or Agency enough time to plan a logical, and cost-effective, implementation. For example, while FIPS 201 allows for the implementation of Part 2 to commence with new employees and contractors first, and allows for the migration of existing credential holders to the new card platform to be accomplished on a phased basis, this will probably result in a situation where redundant badge access systems are required, utilizing two (2) badges. This would be a costly implementation, as it requires the use of multiple systems, with attendant support

and maintenance costs. If the date for FIPS 201, Part 2 compliance is fixed at 10/27/06, DOJ would likely be forced into this costly transitional investment.

Issues of Secondary Concern:

1) HSPD-12 requires that the PIV-II credential have a maximum life of 5 years, and that at re-issuance the credential holder's file be checked to verify that it contains a valid NACI. OPM identified at the HSPD-12 Implementation Workshop held on May 4 & 5, that there is a system limitation for storage of NACI results of 16 years; this time period would need to be extended in order for compliance with the re-issuance process.

2) Page 3, Item 1.B; FIPS 201 identifies that HSPD-12 shall apply to all long-term employees or contractors of the Department or Agency, and this section of the Guidance reaffirms this. However, there has been no definition as to what "long-term" or "short-term" means, and no specific guidance to the Departments or Agencies in making this determination. In addition, the phrase "occasional visitor" is used, and differentiated from short-term guests, but there is no guidance for making this determination. Please add language to this section of the Guidance document to clarify.

3) Page 4, Item 2.A; It is identified that Special Publication 800-76 will be published in its final version on 4/29/05, yet a finalized version of this document has not yet been released. Please provide a revised release date for the final version of this publication.

4) Page 5, Item B; Both FIPS 201 and the Guidance document identify that the background investigation for issuance of personal identity verification (PIV) credentials must be a NACI, "or other Office of Personal Management" investigations, yet in neither document is it defined what is meant by these other OPM investigations. It would be helpful to the Department or Agency if the "other" background investigations that would be compliant with FIPS 201 were delineated in the Guidance document.

5) Page 5, Item C; This paragraph states that language is to be inserted into contracts with private sector companies, whose employees would receive personal identity verification credentials, yet it does not identify what this language is, nor what purpose it is to serve. As the paragraph states that additional information will be included in a FAR amendment, it is recommended that Item C be removed in its entirety, as when the FAR is amended, it will be applicable to all government contracts, and Departments and Agencies will be required to comply at that time.

6) Page 6, Part 1, Item E; This paragraph identifies that those Departments or Agencies with the ability to electronically verify PIV-I credentials, have mechanisms in place to take advantage of this capability in a manner that allows for rapid authentication of the credential. Rapid authentication is defined as the

ability to check if the identity credential is valid "without undue delay". This language is vague, and it is requested that OMB provide specific guidance regarding what constitutes "without undue delay", so as to guide the Department or Agency's technical architecture development.

7) Page 6, Part 2, Item E; This paragraph deals with systems access, and identifies that the Standard requires the activation of at least one digital certificate on the identity credential for access control. However, the language in FIPS 201 clearly states that the use of the PIV credential for physical access and logical systems access is to be determined by the Department or Agency, even though Section 4.3 of FIPS 201 identifies that the card "must store one asymmetric private key and a corresponding public key certificate" to support card authentication. If in fact it is the intention of the Department of Commerce and OMB to require that the PIV credential be used for physical and logical access, the language in FIPS 201 should be amended to reflect this, and the Guidance document should clearly state this requirement. Otherwise, the value of requiring the existence of a certificate, while making its use optional is confusing.

8) Page 8, Item E; To the second sentence, add the phrase ", at a minimum," after "Departments and Agencies are encouraged to use", and before "Standard Form 85"…

9) Page 8, Item 6.A; Both FIPS 201 and the Guidance document already talk to the background investigations required for compliance, so it is unclear what purpose this paragraph serves. As such, it is recommended that this paragraph be deleted.

10) Page 9, Item C; First line, add the word "be" before the word "issued".