USAID Comments
OMB Draft Department and Agency Implementation Guidance for Homeland Security Presidential Directive 12 (HSPD-12), version 4/8/2005

We have the following questions:

1. Re: Section 1.B, p. 3. Does HSPD-12 apply to institutional contractors who don't work in federal agency space, but access and use the agency's network?

2. Re: Section 1.B, p. 3. Does HSPD-12 cover contractors who work in rented space paid for by the agency?

3. The guidance in 1.B (p. 3) states that agencies may decide that the directive does not apply to "other agency specific categories of individuals." Does this mean that the agency could exempt individuals working under Participating Agency Service Agreement (PASAs), Resources Support Services Agreements (RSSAs), Cooperative Administrative Support Units (CASUs), etc? Since these categories of individuals may require access to the agency General Support System (GSS) or information system, they will ultimately need credentials. This guidance appears contradictory.

4. The guidance in 1.B (p. 3) also states that the directive does not apply to short-term guests and occasional visitors and appears to permit the agency to assign these persons temporary identification. Does this create a dual credential system? Similarly, to question 1, if they require access to the agency GSS or information system, they will ultimately need credentials.

5. For 1.C, p. 3, the guidance makes no provision for the duration of the leased space. For short-term leases, would the Directive require that the agency employ electronic readers for credential verification?

6. For 1.C, p. 3, combining language from the first and second bullet in 1.C, if the approaches are to be controlled, in a leased commercial space, would the Directive require that the elevators, stairwells, etc. be secured electronically using the credentials?

7. For 1.D, p. 4, do the requirements of the Directive apply to information systems operated and owned by contractors, but used under contract to the agency?

8. For 1.D, p. 4, if the National Institute of Standards and Technology (NIST) asserts that remote access to federal information systems will require use of

public key infrastructure (PKI) for sensitive data, how can the agency reserve the right to apply the Directive?

9. For 3.A, p. 5, without the ability to currently procure PIV part 2 (PIV-2) compliant cards, how are the agencies to meet the four control objectives as stated in Federal Information Process Standard (FIPS) 201 Section 2.1. Non-PIV-2 compliant cards may not meet control objectives b and c.

10. For 3.B, p. 5, for agencies with foreign nationals, foreign national personal services contractors, and foreign institutional contractors, will there be Department of State procedures for background investigations designated as equivalent to a NACI or Office of Personnel Management (OPM) investigation in time to allow completion of the plan by October 27, 2005?

11. For 3.C, p. 5, do the guidance and Directive apply to contracts which expire after the October 27, 2005 deadline?

12. Within the guidance between 3.D and 3.E, p. 6, the phrase "Departments and agencies whose identity credentials can be verified electronically." (Emphasis added.) Should the term "can" be "must"? If not, is this contradictory?

13. For 3.E, p. 6, what constitutes "undue delay?"

14. For Part 2 A, p. 6, to meet the stated guidance for fully valid interoperable, credentials issued by all agencies must be fully interoperable by October 27, 2006. Is this statement correct? Would there be a dual credential system for personnel with older non-PIV compliant credentials assigned to other agencies?

15. For Part 2 B, p. 6, are OMB, NIST and others going to provide additional technical guidance for interoperability?

16. To comply with the deadline in Part 2 D, p. 6, presuming a National Agency Check and Inquiries (NACI) or equivalent investigation, if a NACI is to be performed for all personnel, does this not establish the final date for conversion to PIV-2 compliant credentials?

17. For 4.A, p. 7, which will GSA and Department of Commerce (DoC)/NIST establish the process for compliance validation for PIV-compliant technologies?

18. Re: Section 5 (Privacy), p. 7. What data on the identity credential (badge) will be readable by means of radio frequency identification (RFID)?

19. NIST Special Publication 800-73, "Appendix A – PIV Process": In A.2 of Appendix A, page 57, it states: "Organizations that possess an automated

identity management system may choose to employ the system based identity proofing, registration, and issuance process set." What kinds of systems would qualify as being "automated identity management systems?" Can agencies that have only partially automated systems fit within this definition, or must an agency's personal identity verification (PIV) system be fully automated?