NASA's Comments on OMB HSPD-12 Implementation Guidance Draft of 8 April 2005

Section 1.A., page 3 – Add the following:… "Department and Agency heads must properly investigate and adjudicate individuals who will be receiving ID credentials."

Section 1.B., page 3 – If an individual will not be visiting other government agencies, and/or accessing IT systems, does s/he have to be vetted and receive a PIV card? More specificity needs to be provided on this section so individuals may be appropriately credentialed.

Section 1.B., 2nd bullet, page 3 – A definitive period of time must be given for "long-term access."

Section 1.B., 4th bullet, page 3 – Why does OMB allow short-term "guest" access to facilities and IT systems without proper vetting? A definitive period of time needs to be given for "short-term." Is this one day, or 1 year?

Section 2.A, Items 2,3,4 in Table, Page 4 – The dates for release of FIPS 201 related technical specifications SP800-73 and 800-76, reference implementations and conformance testing information do not give smart card vendors sufficient time to evolve their products to meet the requirement that agencies comply by 27 October 2006. Although stipulations have been made in 800-73 for a transition card, the interface requirements for the PIV-II card are still beyond the capabilities of the currently available GSC-IS 2.1 compliant products. NASA recommends that the implementation guidance be brought in line with currently available NIST SP 800-73 Part 2 compliant products and that a three to five year transition period be permitted so that the smart card vendors can make the necessary enhancements and agencies accurately budget for the NIST SP 800-73 Part 3 specifications; rather than impose requirements that cannot be met by providers of materials and services. With no delay Agencies may issue current GSC-IS 2.1 FIPS 140 validated cards and applets with the NIST SP 800-73 Part 1 PIV Data Model also compliant with NIST SP 800-73 Part 2. Agencies will not issue these cards without clear guidance that these cards may serve through their nominal 3-5 year life cycle. Within 12 months of availability for NIST SP 800-73 Part 3 compliant products Agencies would convert to issuing only end state cards. This would result in a mixed card population, accommodated by middleware, for a period of 3-5 years following the introduction of the end state cards. Without this approach Agencies, including NASA, will wait until end state cards are available before issuing cards that would need to be replaced before the end of their nominal life cycle.

Section 2.B, Item 4 in Table, Page 4 – The time frame for implementing Part 2 of FIPS 201 is unrealistic because vendors will not able to provide FIPS validated products for implementation by agencies by 27 October 2006. It takes a vendor at least six and as many as twelve months to complete the conformance testing for FIPS accreditation, thus products will not be available for purchase by agencies in a timely enough fashion. NASA recommends that OMB redefine compliance with FIPS 201 Part 2 to mean that by October 2006 an agency has provided employees and on-site contractors with PKI and has submitted a plan to roll-out smart cards to them when vendor products become available in sufficient quantities.

Section 2.C, Item 2 in Table, Page 5 – GSA should oversee and maintain the list of approved authentication products and services that meet the FIPS-201 requirements; however, they are not, and should not be construed as, the only agency from which these can be procured. This is not just a GSA activity. See NASA comments below on Section 4. B for more details.

Section 2.C, Item 3 in Table, Page 5 – GSA does not by itself issue amendments to Federal Acquisition Regulations (FAR). There is an executive committee consisting of members from DoD, GSA and NASA that make these determinations. Once again, too much apparent authority is being attributed to GSA. NASA recommends that OMB change the guidance to more accurately reflect the way changes are made to the FAR.

Section 3, Part 1.A, Page 5 – By October 2005 agencies are required to satisfy the control objective defined in Section 2.1 of FIPS 201. However, the FAR will not be modified until the same time. How can an agency levy requirements on their contractors before the FAR is modified to require NAC or NACI on contractors?

Section 3, Part 1.A, Page 5 – Contracts written prior to this FAR change will not have the NAC or NACI requirements. Will these contracts have to be renegotiated to include them? Will sufficient time be allotted in order for these contracts to be modified, if required?

Section 3, Part 1.A, Page 5 – If current contracts need to be modified in order to comply with the control objectives in Section 2.2 of FIPS 201, will additional funds be allocated for these changes?

Section 3, Part 1.A, Page 5 – If contract changes are required, modifying existing contracts is a costly and time consuming effort. Agencies will most likely not have included these items in their FY06 and FY07 budget submissions to OMB. Will OMB allow agencies to modify their 300Bs in order to include them?

Section 3, Part 1.B, Page 5 – To whom should an agency submit their registration processes for accrediting? Is there a specific format like the PKI Certificate Policy and Certification Practices Framework given in Internet Engineering Task Force Request For Comment Number 3647? Must an agency have their identity proofing process approved before they submit their implementation plan to OMB? NASA recommends that OMB state how these registration processes are accredited, by whom, and in what format an agency should submit them.

Section 3, Part 1.C, Page 5 – An agency can't include proper FIPS-201 language in their contracts until the FAR amendment has been approved. Will this change occur in a timely enough fashion for an agency to modify its contracting language by 27 October 2005? NASA recommends that OMB change this Section to indicate that the FAR change must be in place before the agencies can include this language.

Section 3, Part 1.E, Page 6 – The ability to rapidly authenticate credentials is not included in Part 1 of FIPS-201. NASA recommends this Section be deleted or moved to Part 2.

Section 3, Part 2.B, Page 6 – This is only possible if NIST SP 800-73 Part 2 Cards deployed during the initial period of deployment.

Section 3, Part 2.D, Page 6 – What does OMB mean by the statement, "**By September 30, 2007, identity proofing should be on record for all current employees and contractors.**"? This contradicts FIPS 201 policy (ref §2.2). Furthermore, EO 10450, 5CFR731 & 5CFR732 do not currently require NAC or NACI investigations for all contract employees. NASA's

employee base is nearly 80% contractors. Completion of a NAC/NACI on all contractors within the specified time is unachievable.

Section 4,B. Page 7, – Setting up GSA as "an executive agent for Government-wide acquisitions of information technology", as stated in Section 4. B. gives the impression of too much authority to GSA for the purchase of the authentication products and services required by FIPS 201. GSA is one of many agencies that already have statutory authority for Government Wide Acquisition Contracts (GWAC). For example, NASA has a Scientific Engineering Workstation Procurement (SEWP) GWAC. The software and hardware products needed to comply with FIPS- 201 are already available from the NASA SEWP III contract. NASA recommends that GSA not be the only agency mentioned.

Section 4,B. Page 7, – The March 15, 2005, date preceded the release of the OMB guidance. Furthermore, there are substantial problems with the handbook. The FICC should be given sufficient time, until at least July 15, 2005, to promulgate the final version of the handbook.

Section 4., Page 7, - Over standardization of card topology will lull government guard forces into complacency. One of the control objectives in HSPD 12 is for PIV card to be, "*rapidly authenticated electronically*". Card topology should be at the department/agency's discretion. FIPS 201, and associated special publications, provides a cookbook approach for counterfeiting Federal credentials. Emphasis should be on electronic verification, and not card topology/design.

Section 6.A. Page 8 – This Section only covers civil servants. NASA recommends that it be expanded to cover contractors as well.

Section 7.A., pages 8 & 9, - OMB requires agencies to send sensitive but unclassified information to OMB via electronic mail. NASA recommends that OMB provide a more secure means for transmitting the information.