Subject: VA comments to FIPS 201
From: "Catoe, Fred" <fred.catoe@va.gov>
To: <draftfips201@nist.gov>
Cc: <Tim.Polk@nist.gov>

Here are VA's comments. VA would like to schedule a meeting with NIST in January to discuss our concerns. Please let me know who I should contract concerning a meeting.

If you have any questions, please contact Fred Catoe at 202-273-8122.

Department of Veterans Affairs
Formal Response to FIPS 201 Public Draft

In accordance with the guidance contained in the public draft of FIPS 201, Personal Identity Verification (PIV) for Federal Employees and Contractors, the Department of Veterans Affairs (VA) is hereby submitting our comments electronically in accordance with the public draft instructions.

In principal, VA supports the mandates in HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*. At the same time the schedule called for is aggressive and may create an environment where proper due diligence is difficult to achieve. VA has concerns that the costs required to implement the provisions of the FIPS 201 public draft will not be balanced against the benefits or the perceived risks that this document intends to mitigate.

On December 16, 2004 VA participated in a meeting of the Smart Card Manager's Interagency Advisory Board (IAB) to review an alternative version of FIPS 201. While VA still has certain concerns, which are addressed below, the Department voted to support the IAB version in place of the original NIST public draft. This vote of support was offered "with reservations." Therefore, the comments contained in this response are predicated on the IAB draft as of December 16, 2004, and contain areas where VA is still not comfortable. However, VA wishes to concentrate our comments on key issues versus specific details where we have concerns.

Over the past couple of years VA has been very active in the field of smart cards, public key infrastructure (PKI) and Identity and Access Management (IAM) solutions. This includes our involvement in areas such as E-Authentication and the Federal Identity Credentialing Committee. Government and industry have taken notice of the competency and technical approach VA is taking in our Authentication and Authorization Infrastructure Project (AAIP), which incorporates smart card technologies as part of our One-VA ID card. Today, AAIP is in the Limited Deployment Phase, giving VA an informed opinion on the requirements, issues and risks associated with the mandates of FIPS 201. As such, VA is offering our perspective on FIPS 201 using our experience and expertise in this area.

**Human Resource/Contractor Processes**
VA believes that the timeline for Human Resources to process a new employee, or for contractors to be fully processed will adversely impact our organization. Currently, VA has approximately 80,000 new individuals active in our healthcare system through our association with teaching universities. The processes defined may prove to be so onerous that VA may have difficulties in sustaining these programs. This will result in significant disruption to VA healthcare, and will raise costs.

The current position of FIPS 201 would preclude VA from employing a healthcare clinician until they complete a security clearance. From VA's perspective, this will have a devasting impact on available medical services for our veterans, who are principally concerned that a doctor holds appropriate medical credentials versus the security clearance of their doctors.

VA recommends consideration of graduated processes that take into account the benefits derived against the disruption that will occur in organizations such as VA. Again, VA does not believe that a single approach without certain latitudes serves the interests of government and our constituents.

**Biometrics**

VA believes that the intent of FIPS 201, as drafted in the original format and in the IAB format mandates biometrics that will create significant cost and privacy issues. VA has asked for a business case related to both versions of FIPS 201, but has yet to receive one. VA rejects the assertion that biometrics is the only way to achieve the mandates of HSPD-12, especially where the biometrics are not required to be digitally signed to assure integrity. VA also has concerns that federal standards have not been adopted, and are not expected to be adopted prior to February 25, 2005 when FIPS 201 will be officially published.

The IAB version of FIPS 201 will require the implementation of a biometric repository to support a mandatory one-to-many search of biometric data during enrollment of an individual. VA questions whether the cost can be justified, and whether technology exists to do everything that will be mandated in the FIPS document. A summary analysis by VA indicates that the cost impact will be substantial – tens of millions of dollars, and at the same time our constituents – the nation's veterans – will derive no direct benefit. Additionally, VA wishes to point out that the current draft versions of FIPS 201 do not properly address privacy concerns, and our labor unions have already raised challenges to the incorporation of fingerprint based biometrics into AAIP. Further, during detailed analysis during the Prototype Phase of AAIP, VA was unable to identify business or risk mitigation benefits related to the use of biometrics in most of VA's facilities. Except in limited cases, biometrics is not properly suited to VA's operational environment.

VA recommends that alternative approaches be considered, and where biometrics is still considered to be the best technical solution to achieve HSPD-12 that a proper business case be formulated. The business case must take into consideration privacy concerns, and should identify graduated security levels where biometrics would be required. If required by law, this provision of FIPS 201 may require a cost impact analysis.

**Smart Card Storage**

VA has significant concerns that the available memory on a 64K smart card will not support all of the FIPS mandated contents and still be able to support VA business requirements. VA currently has a two certificate model, while FIPS 201 points towards a three certificate model plus the incorporation of a separate personnel identity verification (PIV) certificate and mandatory biometric data. VA has a business requirement to incorporate a Drug Enforcement Agency (DEA) digital certificate to support automated pharmacy transactions, and we would like to be able to store the previous encryption certificate to minimize key recovery efforts.

VA recommends that NIST conduct an analysis of projected storage requirements, and make this analysis known to the federal agencies for consideration and further comment.

**Objectives and Criteria**

FIPS 201 should be highly focused on establishing objectives and criteria that allows each federal agency to tailor their implementations. The appropriate implementation at VA is likely to be substantially different than the implementation considerations and requirements of a small federal agency. The current draft does not take this into account, and will raise complexity and costs across government.

The IAB version of FIPS 201 moves towards this by reducing the total number of roles involved in the issuance of a credential to an employee. In the original version there are five separate roles which increases the total number of individuals involved in the AAIP process by at least 20 percent – representing millions of dollars in costs annually. VA would like to see more of the IAB version leverage this approach.

VA recommends that the FIPS 201 draft incorporate language that ensures flexible implementations without

compromising the objectives and criteria that each agency should use to measure the success of their programs.

**Internal Data Systems and Architecture**

VA believes that FIPS 201 will require each agency to create new data system to support the process requirements identified in the draft. VA has three principal concerns. Federal agencies will not leverage the efforts of other agencies, creating duplicate cost. Secondly, several of these new data systems will contain information protected under the Privacy Act. As such, each agency will be required to publish notice as required for a "System of Record" in accordance with federal law. Third, the requirements of FIPS 201 will mandate that every agency incorporate public key technology (PKI) into their architectures, and the technical components such as the requirement to implement Online Certificate Status Protocol (OCSP) are directly contrary to the current federal requirements contained in the Common Certificate Policy published through the FICC.

VA also wishes to point out that FIPS 201 will require an additional step to verify that a credential is valid, creating new costs and impacts – and these are significant costs that are not fully accounted for, potentially raising costs for VA's AAIP program by . This includes credentials such as State drivers licenses. To comply with this requirement, each of the agencies will have to coordinate with each State agency to establish procedures and working relations. Each agency will have to interact with State agencies for every single enrollment process. This creates duplicative effort which runs contrary to efficient government. VA is also concerned that the States will treat this as an opportunity to generate revenue through new fees to address the new workload.

VA recommends that OMB identify an appropriate forum or mechanism for agencies to leverage work related to creation of such new data systems and that OMB start actions now to provide authorization for federal agencies to create the "System of Record" solutions that will be required to implement FIPS 201. VA would like to have alignment of the PKI aspects to correct inconsistencies with the federal Common Certificate Policy managed through the FICC. Further, OMB should identify how the federal agencies will work with the States.

**Interoperability**

VA believes that the intent of FIPS 201, as drafted in both the original and IAB format cannot be achieved in a cost effective manner without significant attention to interoperability across government agencies. It is not prudent to require a common solution for government, but leave architecture, implementation and management up to each individual agency. Further, VA understands that no new funding will be provided to address FIPS 201 requirements.

VA recommends that OMB identify a federal resource to coordinate a common interoperable architecture, implementation details and management of common system(s) required in FIPS 201 in a cost effective manner. A federal budget should be established and funded to support this activity.

**GPEA Conflict**

VA believes that the mandates in FIPS 201 will result in numerous cases where federal agencies have to implement new manual processes, either short-term or long-term. These processes may in fact create a conflict with the Government Paperwork Elimination Act (GPEA).

VA requests OMB to consider the impact of FIPS 201 and determine if there is a legal conflict, or whether specific guidance needs to be issued to federal agencies to assist them in avoiding a conflict with GPEA.

The Department of Veterans Affairs appreciates the opportunity to comment, and share our expertise in this area. While VA supports the mandates of HSPD-12, we believe that the implementation details contained in

FIPS 201 and the pending review of NIST Special Publication 800-73 should balance the benefits, the state of technology, and the risks to be mitigated to protect what will turn out to be an expensive investment by the government.

 VA Response to FIPS 2014.DOC

Department of Veterans Affairs
Formal Response to FIPS 201 Public Draft

In accordance with the guidance contained in the public draft of FIPS 201, Personal Identity Verification (PIV) for Federal Employees and Contractors, the Department of Veterans Affairs (VA) is hereby submitting our comments electronically in accordance with the public draft instructions.

In principal, VA supports the mandates in HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors.* At the same time the schedule called for is aggressive and may create an environment where proper due diligence is difficult to achieve. VA has concerns that the costs required to implement the provisions of the FIPS 201 public draft will not be balanced against the benefits or the perceived risks that this document intends to mitigate.

On December 16, 2004 VA participated in a meeting of the Smart Card Manager's Interagency Advisory Board (IAB) to review an alternative version of FIPS 201. While VA still has certain concerns, which are addressed below, the Department voted to support the IAB version in place of the original NIST public draft. This vote of support was offered "with reservations." Therefore, the comments contained in this response are predicated on the IAB draft as of December 16, 2004, and contain areas where VA is still not comfortable. However, VA wishes to concentrate our comments on key issues versus specific details where we have concerns.

Over the past couple of years VA has been very active in the field of smart cards, public key infrastructure (PKI) and Identity and Access Management (IAM) solutions. This includes our involvement in areas such as E-Authentication and the Federal Identity Credentialing Committee. Government and industry have taken notice of the competency and technical approach VA is taking in our Authentication and Authorization Infrastructure Project (AAIP), which incorporates smart card technologies as part of our One-VA ID card. Today, AAIP is in the Limited Deployment Phase, giving VA an informed opinion on the requirements, issues and risks associated with the mandates of FIPS 201. As such, VA is offering our perspective on FIPS 201 using our experience and expertise in this area.

**Human Resource/Contractor Processes**

VA believes that the timeline for Human Resources to process a new employee, or for contractors to be fully processed will adversely impact our organization. Currently, VA has approximately 80,000 new individuals active in our healthcare system through our association with teaching universities. The processes defined may prove to be so onerous that VA may have difficulties in sustaining these programs. This will result in significant disruption to VA healthcare, and will raise costs.

The current position of FIPS 201 would preclude VA from employing a healthcare clinician until they complete a security clearance. From VA's perspective, this will have a devasting impact on available medical services for our veterans, who are principally concerned that a doctor holds appropriate medical credentials versus the security clearance of their doctors.

VA recommends consideration of graduated processes that take into account the benefits derived against the disruption that will occur in organizations such as VA. Again, VA does not believe that a single approach without certain latitudes serves the interests of government and our constituents.

**Biometrics**

VA believes that the intent of FIPS 201, as drafted in the original format and in the IAB format mandates biometrics that will create significant cost and privacy issues. VA has asked for a business case related to both versions of FIPS 201, but has yet to receive one. VA rejects the assertion that biometrics is the only way to achieve the mandates of HSPD-12, especially where the biometrics are not required to be digitally signed to assure integrity. VA also has concerns that federal standards have not been adopted, and are not expected to be adopted prior to February 25, 2005 when FIPS 201 will be officially published.

The IAB version of FIPS 201 will require the implementation of a biometric repository to support a mandatory one-to-many search of biometric data during enrollment of an individual. VA questions whether the cost can be justified, and whether technology exists to do everything that will be mandated in the FIPS document. A summary analysis by VA indicates that the cost impact will be substantial – tens of millions of dollars, and at the same time our constituents – the nation's veterans – will derive no direct benefit. Additionally, VA wishes to point out that the current draft versions of FIPS 201 do not properly address privacy concerns, and our labor unions have already raised challenges to the incorporation of fingerprint based biometrics into AAIP. Further, during detailed analysis during the Prototype Phase of AAIP, VA was unable to identify business or risk mitigation benefits related to the use of biometrics in most of VA's facilities. Except in limited cases, biometrics is not properly suited to VA's operational environment.

VA recommends that alternative approaches be considered, and where biometrics is still considered to be the best technical solution to achieve HSPD-12 that a proper business case be formulated. The business case must take into consideration privacy concerns, and should identify graduated security levels where biometrics would be required. If required by law, this provision of FIPS 201 may require a cost impact analysis.

**Smart Card Storage**

VA has significant concerns that the available memory on a 64K smart card will not support all of the FIPS mandated contents and still be able to support VA business requirements. VA currently has a two certificate model, while FIPS 201 points towards a three certificate model plus the incorporation of a separate personnel identity verification (PIV) certificate and mandatory biometric data. VA has a business requirement to incorporate a Drug Enforcement Agency (DEA) digital certificate to support automated pharmacy transactions, and we would like to be able to store the previous encryption certificate to minimize key recovery efforts.

VA recommends that NIST conduct an analysis of projected storage requirements, and make this analysis known to the federal agencies for consideration and further comment.

**Objectives and Criteria**

FIPS 201 should be highly focused on establishing objectives and criteria that allows each federal agency to tailor their implementations. The appropriate implementation at VA is likely to be substantially different than the implementation considerations and requirements of a small federal agency. The current draft does not take this into account, and will raise complexity and costs across government.

The IAB version of FIPS 201 moves towards this by reducing the total number of roles involved in the issuance of a credential to an employee. In the original version there are five separate roles which increases the total number of individuals involved in the AAIP process by at least 20 percent – representing millions of dollars in costs annually. VA would like to see more of the IAB version leverage this approach.

VA recommends that the FIPS 201 draft incorporate language that ensures flexible implementations without compromising the objectives and criteria that each agency should use to measure the success of their programs.

**Internal Data Systems and Architecture**

VA believes that FIPS 201 will require each agency to create new data system to support the process requirements identified in the draft. VA has three principal concerns. Federal agencies will not leverage the efforts of other agencies, creating duplicate cost. Secondly, several of these new data systems will contain information protected under the Privacy Act. As such, each agency will be required to publish notice as required for a "System of Record" in accordance with federal law. Third, the requirements of FIPS 201 will mandate that every agency incorporate public key technology (PKI) into their architectures, and the technical components such as the requirement to implement Online Certificate Status Protocol (OCSP) are directly contrary to the current federal requirements contained in the Common Certificate Policy published through the FICC.

VA also wishes to point out that FIPS 201 will require an additional step to verify that a credential is valid, creating new costs and impacts – and these are significant costs that are not fully accounted for, potentially raising costs for VA's AAIP program by . This includes credentials such as State drivers licenses. To comply with this requirement, each of the agencies will have to coordinate with each State agency to establish procedures and working relations. Each agency will have to interact with State agencies for every single enrollment process. This creates duplicative effort which runs contrary to efficient government. VA is also concerned that the States will treat this as an opportunity to generate revenue through new fees to address the new workload.

VA recommends that OMB identify an appropriate forum or mechanism for agencies to leverage work related to creation of such new data systems and that OMB start actions now to provide authorization for federal agencies to create the "System of Record" solutions that will be required to implement FIPS 201. VA would like to have alignment of the PKI aspects to correct inconsistencies with the federal Common Certificate Policy managed through the FICC. Further, OMB should identify how the federal agencies will work with the States.

**Interoperability**

VA believes that the intent of FIPS 201, as drafted in both the original and IAB format cannot be achieved in a cost effective manner without significant attention to interoperability across government agencies. It is not prudent to require a common solution for government, but leave architecture, implementation and management up to each individual agency. Further, VA understands that no new funding will be provided to address FIPS 201 requirements.

VA recommends that OMB identify a federal resource to coordinate a common interoperable architecture, implementation details and management of common system(s) required in FIPS 201 in a cost effective manner. A federal budget should be established and funded to support this activity.

**GPEA Conflict**

VA believes that the mandates in FIPS 201 will result in numerous cases where federal agencies have to implement new manual processes, either short-term or long-term. These processes may in fact create a conflict with the Government Paperwork Elimination Act (GPEA).

VA requests OMB to consider the impact of FIPS 201 and determine if there is a legal conflict, or whether specific guidance needs to be issued to federal agencies to assist them in avoiding a conflict with GPEA.

The Department of Veterans Affairs appreciates the opportunity to comment, and share our expertise in this area. While VA supports the mandates of HSPD-12, we believe that the implementation details contained in FIPS 201 and the pending review of NIST Special Publication 800-73 should balance the benefits, the state of technology, and the risks to be mitigated to protect what will turn out to be an expensive investment by the government.