Subject: Comments on Public Draft FIPS 201
From: "Diana Manfredi" <dmanfredi@saflink.com>
To: <draftFIPS201@nist.gov>

Dear Curt,

Attached please find SAFLINK Corp's comments on the public draft of FIPS 201. Unfortunately, I just noticed that a newer file was uploaded on Dec 20th - our reviewers may have used a version for comments post Nov 8th, but not necessarily post Dec 20th. Hopefully our comments still align. Please feel free to contact me at any time.

Regards,
Diana Manfredi

---

For a closer look at our products and services please see our website www.saflink.com

---


Diana Demo Manfredi
Project Manager
SAFLINK Corporation
1875 Campus Commons Dr., Suite 301
Reston, VA 20191
703.547.0187
dmanfredi@saflink.com

---



SAFLINK Comments-FIPS201-12222004.xls

| Cmt # | Organization | Point of Contact | Comment Type (G-General, E-Editorial, T-Technical) | Section,Annex,etc and Page Nbr | Comment(Include rationale for comment) | Proposed change |
|---|---|---|---|---|---|---|
| 1 | SAFLINK | Diana Manfredi | E | 1.2, para 1, line 2 (page 1) | Clarification | Change "established the requirements for a common identification standard for identification issued" to "established the requirements for a common identification standard for identification **credentials** issued" |
| 2 | SAFLINK | Diana Manfredi | G | Sec. 1.3; second paragraph (page 2) | This Section should be expanded to make it clearer that an agency has the discretion to implement other biometric technologies (such as iris and hand geometry) or other formats of biometric identifiers (such as fingerprint templates) for agency-specific applications. For example, in certain applications where fingerprints may not be practical (e.g., protective gloves are required), iris recognition may be used for authentication. Also, for door access systems that are exposed to the weather, hand geometry devices may be more appropriate due to their higher tolerance for variations in temperature and moisture. | Modify sentence in second paragraph to read: "This standard does not restrict the agencies from adopting additional alternatives, including other biometric technologies and biometric data formats that may be appropriate for specific agency applications." |
| 3 | SAFLINK | Diana Manfredi | G | 2.2.1, para 2 (page 5) | The requirement states that 2 forms of documents from the I-9 are required. It is therefore assumed that this credential will not be issued to Canadian or Mexican citizens who are not living in the US on a visa. Is this correct? (i.e., contractors whose home base is in Canada would not be eligible since they do not have an SSN, alien registration, or visa number) | None. |
| 4 | SAFLINK | Diana Manfredi | E | Table 2-1 (page 6) | Add level names/descriptions to column 1 in addition to the level numbers (as is done in Table 2-2) for clarity and consistency. | Add level names. |
| 5 | SAFLINK | Diana Manfredi | T | 2.2.1, page 6, para below Table 2-1 | Would it not make more sense to capture the facial image/photo at the same time as the fingerprints are collected (i.e., during identity proofing/registration) rather than during credential issuance? | Add requirement to 2.2.1 to capture facial photo. |
| 6 | SAFLINK | Diana Manfredi | T | Table 2-2 | Does each level include all lower level checks in addition to the check indicated? For example, does level 2 (moderate) require source document authentication in addition to NACI? If so this should be explicitly stated. | Add statement regarding each level including all lower level requirements, if appropriate. |

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

| Cmt # | Organization | Point of Contact | Comment Type (G-General, E-Editorial, T-Technical) | Section,Annex,etc and Page Nbr | Comment(Include rationale for comment) | Proposed change |
|---|---|---|---|---|---|---|
| 7 | SAFLINK | Diana Manfredi | T | 2.2.1, page 6, 2nd para & Table 2-2 (+ Annex D) | Is it planned that checks against the TSC (Threat Screening Center) will be performed or is this included as part of one of the other background checks? | None. |
| 8 | SAFLINK | Diana Manfredi | T | 2.2.1, page 5-7 | Will a biometric duplicate check be performed as part of the identity proofing/registration process? (This is implied in other parts of the document, e.g., 4.4.1.) If so, it should be so stated here. | Add requirement to 2.2.1 to perform 1:N duplicate check, if appropriate. |
| 9 | SAFLINK | Diana Manfredi | T | 2.3, para 1 (page 7) | Facial photo is to be taken at time of credential issuance. Would this not be needed during identity registration in order to capture the photo for printing on surface, as well as optional storage of the digital image on the card? (See also related comment on 2.2.1.) | Move requirement for facial photo capture from 2.3 to 2.2.1, if appropriate. |
| 10 | SAFLINK | Diana Manfredi | E | 2.3, para 1, line 5 (page 7) | Typo | Change "(I.e.," to "(i.e.," |
| 11 | SAFLINK | Diana Manfredi | T | 3.3, 1st bullet (page 12) | Would the functional components not also include the platforms these peripherals reside upon? | Add to the end of the 1st sentence ", and the platforms upon which they reside." |
| 12 | SAFLINK | Diana Manfredi | T | Figure 3-1 (page 13) | PIV Card Issuance and Management block: Should "card management system" be included here or is it a sub-element of one of the other blocks (e.g., card issuance)? | Add if appropriate. |
| 13 | SAFLINK | Diana Manfredi | E | 3.3.1, para 4, line 4 (page 14) | Wording | Change "comparison of a ..." to "comparison **to** a ..." |
| 14 | SAFLINK | Diana Manfredi | T | 3.4, bullet #2 (page 16) | The description of Identity proofing and registration does not mention the performance of any biometrics collection or background checks. These seem to be an important element of this area. | Add sentence related to these functions. |
| 15 | SAFLINK | Diana Manfredi | E | 4.1.1.b (page 17) | Clarity | Change "Printed material should not interfere with contact or contactless placement..." to "Printed material should not interfere with contact or contactless **chip** placement ... " or "Printed material should not interfere with contact **chip** or contactless **antenna** placement ..." |

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

| Cmt # | Organization | Point of Contact | Comment Type (G-General, E-Editorial, T-Technical) | Section,Annex,etc and Page Nbr | Comment(Include rationale for comment) | Proposed change |
|---|---|---|---|---|---|---|
| 16 | SAFLINK | Diana Manfredi | E | 4.1.2.b (page 17) | Clarity | Change "and currency of these tamper resistance and anti-couterfeiting methods" to "and currency of **any** tamper resistance and anti-counterfeiting methods **considered.**" |
| 17 | SAFLINK | Diana Manfredi | E | 4.1.3e (page 18) | Clarity | Change "austere" to "severe" when referring to environment as austere could refer to lack of adornment. |
| 18 | SAFLINK | Diana Manfredi | T | 4.1.4.1.a (page 19) | Recommend adding requirement for facial photo capture to follow the guidelines of ANSI INCITS 385. | Add reference. |
| 19 | SAFLINK | Diana Manfredi | T | 4.1.5.1, 2nd para (page 23) | Should an 'external authentication' key also be included as a possible CTC authentication method? | Add, if appropriate. |
| 20 | SAFLINK | Diana Manfredi | T | 4.1.5.2, 1st para, last sentence (page 23/24) | It is assumed that this is refering to the interoperable biometric. If so, it would be better to state for clarity since it is possible that other biometric data could optionally be stored on the card. | Change to "CHUID and **interoperable** biometric information" |
| 21 | SAFLINK | Diana Manfredi | T | 4.2 (page 25) | This section identifies some elements of the CHUID as defined in the PACS guidance documents, but ignores others. Suggest including a table that lists all CHUID entries and indicates which are used and which are unused. [For example, FASC-N is addressed, but agency code, organizational identifier, DUNS, and GUID are not mentioned.] | Add table or state that inclusion of optional CHUID elements are at the discretion of the agency. |
| 22 | SAFLINK | Diana Manfredi | E | Table 4-2 (page 25) | Title should read "CHUID Additional Data Elements" | Correct title of table. |
| 23 | SAFLINK | Diana Manfredi | E | Table 4-3 (page 25) | Expiration Date description is missing the day values. | Change to read "yyyymm**dd**" |
| 24 | SAFLINK | Diana Manfredi | T | 4.2.2 (page 26) | Method of padding of hash values in the signature should be specified. | Specify. |
| 25 | SAFLINK | Diana Manfredi | E | 4.3 (page 28) | Bullet at top of page - Explicitly state that this key optional as is done for all other keys (1st 4 bullets). | Add "optional". |
| 26 | SAFLINK | Diana Manfredi | E | 4.4 (page 30) 1st para after 1st set of bullets, 2nd sentence. | Grammar. | Change "Fingerprints shall be primary biometric" to "Fingerprints shall be **the** primary biometric" |
| 27 | SAFLINK | Diana Manfredi | T | 4.4 , next to last para (page 30) | States that "For PIV, one-to-many fingerprint matching will be performed during the Application process." Does this refer to the criminal background check, internal duplicate check, or both? | Be explicit. |

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

| Cmt # | Organization | Point of Contact | Comment Type (G-General, E-Editorial, T-Technical) | Section,Annex,etc and Page Nbr | Comment(Include rationale for comment) | Proposed change |
|---|---|---|---|---|---|---|
| 28 | SAFLINK | Diana Manfredi | T | 4.4, last para (page 30) | RESUBMIT: Since contactless cards are the primary media for physical access, restricting the reading of biometric data from the contact side only severely limits the use of the interoperable biometric for physical access. | Delete paragraph. |
| 29 | SAFLINK | Diana Manfredi | T | 4.4.1 (page 30) | Use of biometrics for duplicate checking (which implies an internal AFIS system) during issuance is not mentioned in previous sections describing card issuance (e.g., 2.2 & 3.3.2). | Check for consistency. |
| 30 | SAFLINK | Diana Manfredi | T | 4.4.1 (page 30) | The 2nd sentence states "The biometric data supplied for biometric identification search shall consist of a complete set of ten "slap" fingerprints which may alternatively be accompanied by a set of ten rolled fingerprint images." Is this in addition to or in lieu of? | Delete "alternatively". |
| 31 | SAFLINK | Diana Manfredi | G | Sec. 4.4.2; page 31; third & fifth paragraphs | There has been considerable effort invested by NIST, ANSI/INCITS M1, ISO and the biometrics industry in defining fingerprint template interoperability standards. We recommend that FIPS 201 include a statement that these approved template standards represent the preferred approach for interoperability due to their inherent efficiency in a smart card environment. We believe that using fingerprint images will not be practical in some specific applications due to performance considerations. Specifically, the data transfer rate limitations of the contact smart card and the additional time required for decompression and feature extraction of fingerprint images make the use of fingerprint images impractical for applications requiring rapid authentication like physical access control. We recommend that NIST provide guidance to vendors so that they can implement to these tamplate standards in a manner that will achieve interoperability. We recommend that NIST accelerate its testing of template interoperability. | Add the following to the end of the third paragraph: "It is recognized that the use of standard fingerprint templates represent the most efficient approach to achieving interoperability in the PIV environment. It is anticipated that the use of interoperable fingerprint templates will be added to this standard as soon as further testing has been performed." |
| 32 | SAFLINK | Diana Manfredi | E | 4.4.2, 3rd para (page 31) | Neither of the standards (ANSI INCITS 378-2004 and ISO/IEC 19794-2) are included in the references in Annex F. | Add references to Annex F. |

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

| Cmt # | Organization | Point of Contact | Comment Type (G-General, E-Editorial, T-Technical) | Section,Annex,etc and Page Nbr | Comment(Include rationale for comment) | Proposed change |
|---|---|---|---|---|---|---|
| 33 | SAFLINK | Diana Manfredi | E | 4.4.3, 1st para (page 31) | Add reference mark [FFSMT] after the ITL standard. | Check consistency between body and Annex F. |
| 34 | SAFLINK | Diana Manfredi | E | 4.4.3, 1st para (page 31) | Only Annex F of the EFTS spec is included in Annex F. Add reference to main document and add reference mark here. | Check consistency between body and Annex F. |
| 35 | SAFLINK | Diana Manfredi | E | 4.4.3 (page 32), 5th para on this page | Add reference mark [EFTS/F] after reference. | Check consistency between body and Annex F. |
| 36 | SAFLINK | Diana Manfredi | T | 4.4.3, (page 32), 5th para on this page | Include estimated space requirements for the fingerprint image(s). | Add if appropriate. |
| 37 | SAFLINK | Diana Manfredi | T | 4.4.3 (page 32), Next to last para | A compression ratio or range should be specified (e.g., not to exceed 15:1). | Specify compression ratio. |
| 38 | SAFLINK | Diana Manfredi | E | 4.4.3, last para (page 32) | Add reference mark [NFIQUA] after the NISTIR 7151 standard. | Check consistency between body and Annex F. |
| 39 | SAFLINK | Diana Manfredi | T | Sec. 4.4.4; page 34; first paragraph | This Section suggests that two fingerprints must be presented for PIV card authentication. In many applications, presentation of a single fingerprint would be more efficient without measurably detracting from security. We recommend that agencies be given the choice of using one or both fingers depending on their specific application requirements. | Modify the first sentence to read: "This standard requires the capture of one or two fingerprint images for the purpose of PIV card authentication."<br><br>Modify the next to last sentence to read: "At the authentication station, one or two fingerprints shall be captured." |
| 40 | SAFLINK | Diana Manfredi | E | 4.4.4, 2nd para (page 34) | The reference [NISTIR 6529-2001] is included but is not present in Annex F. | Check consistency between body and Annex F. |
| 41 | SAFLINK | Diana Manfredi | E | 4.4.4, 2nd para (page 34) | Add reference mark [FIBIF] after ANSI INCITS 381-2004. | Check consistency between body and Annex F. |
| 42 | SAFLINK | Diana Manfredi | T | 4.4.4, 2nd para (page 34) | Should a specific CBEFF patron format be called out? A list of CBEFF header elements is included in 4.4.6, but is more appropriate here. | Add patron format, if desired. Move CBEFF header elements from 4.4.6 here. |
| 43 | SAFLINK | Diana Manfredi | E | 4.4.4, 2nd para (page 34) | 2nd sentence states "The fingerprint records generated for PIV card approval will be ...". What does "for PIV card approval" mean in this context? | Delete "for PIV card approval" or be more specific about the process step intended. |
| 44 | SAFLINK | Diana Manfredi | E | 4.4.5 (page 35) | Para under bullets - Add reference mark [FRFD] after ANSI INCITS 385-2004]. | Check consistency between body and Annex F. |

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

| Cmt # | Organization | Point of Contact | Comment Type (G-General, E-Editorial, T-Technical) | Section,Annex,etc and Page Nbr | Comment(Include rationale for comment) | Proposed change |
|---|---|---|---|---|---|---|
| 45 | SAFLINK | Diana Manfredi | T | 4.4.5 (page 35) | Use of the token facial image implies that the digital representation of the face is to be stored on the card. If so, then it must be collected during registration/enrollment as opposed to during card issuance as indicated in 2.3. | Specify facial image must be captured at same time as fingerprints. |
| 46 | SAFLINK | Diana Manfredi | T | 4.4.5 (page 35) | Include estimated space requirements for the facial image. | Add if appropriate. |
| 47 | SAFLINK | Diana Manfredi | E | 4.4.5.5, 1st sentence (page 35) | The wording of this sentence is not in specification language. | Change to read "Because PIV cards are likely to have limited storage space and face recognition performance has been demonstrated to be sensitive to compression ratio ([NISTIR 7083], **these factors must be balanced when determining the** compression ratio. |
| 48 | SAFLINK | Diana Manfredi | T | Figure 4-4 (page 36) | Figure implies regional compression, but text and Table 4-7 state 30:1 only. | Clarify. |
| 49 | SAFLINK | Diana Manfredi | E | 4.4.6 (page 37-38) | CBEFF header elements should be specified in 4.4.4. This section should merely indicate that the CBEFF header is included in the signature. | Change to read: The digital signature shall be computed over the concatenation of the following CBEFF elements: - CBEFF Header - BSMB. |
| 50 | SAFLINK | Diana Manfredi | T | 4.5.2 (page 39) | RESUBMIT: This paragraph should specify whether 14443 A or B or both are required. | Add, if appropriate. |
| 51 | SAFLINK | Diana Manfredi | T | 4.5.3, 1st sentence (page 39) | The term 'activated' may be incorrectly used here. Consider replacing with 'opened'. Also, check for correct use of term in other parts of the document. | Change to read "PIV cards may be **opened** through the contact interface ..." |
| 52 | SAFLINK | Diana Manfredi | G | 5 (page 40) | How will certs be issued such that they will be usable for logical access across organizations/domains? | None. |
| 53 | SAFLINK | Diana Manfredi | T | 5.1.2 (page 40) | What process will be used for revoking the cards? Will this only entail revoking the certificates? If so, this will be a problem in the physical access environment (in which cryptography at the door may not be feasible). | Consider adding a section on card revocation. [Alternate mechanisms to be considered include bad card lists.] |
| 54 | SAFLINK | Diana Manfredi | G | 5 | There does not appear to be a section describing card reissuance. This should be included. | Add, if appropriate. |
| 55 | SAFLINK | Diana Manfredi | E | 5.2.1 (page 40-42) | Much of the text in this section is repetive of section 2.2. Suggest keeping high level information in early section and details here. (For example tables 5-1 and 5-2 are probably more appropriate here than as 2-1 and 2-2. In any event - once is enough.) | Delete repetitive material. |

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

| Cmt # | Organization | Point of Contact | Comment Type (G-General, E-Editorial, T-Technical) | Section,Annex,etc and Page Nbr | Comment(Include rationale for comment) | Proposed change |
|---|---|---|---|---|---|---|
| 56 | SAFLINK | Diana Manfredi | T | 5.2.1 (page 41) | Last sentence on this page states: "The registration authority may optionally also photograph the Applicant for personalization of the PIV card." It is agreed that this is the correct time to perform the photo capture, but this conflicts with previous sections. Also, wouldn't this be required (as opposed to optional) in order to meet the topology requirements of 4.1.4.1? | No change here, but should change previous (2.2.1 and 2.3) sections to be consistent. |
| 57 | SAFLINK | Diana Manfredi | T | 5.2.2 (page 42) | This implies that each biometric record is signed (ala CBEFF optional digital signature), but 4.4.6 implies that an external signature is to be used. | Check consistency to clarify if the record or container is to be signed. Add to end of 2nd sentence ", as specified in 4.4.6." |
| 58 | SAFLINK | Diana Manfredi | T | 5.2.2, 2nd para (page 43) | This section indicates that the applicant may generate cryptographic key pairs. The generation of keypairs under the control of the user could put the keys at risk of comporomise or the keys could be intentionally compromised by generating them in a software device or on insecure and uncertified hardware. | Consider adding text addressing the security issues of applicant generated keys and ways to mitigating risk. Recommend that key generation happen under the control of the RA or Card Managment System using the card management keys to ensure that keys are generated on the token and cannot be compromised |
| 59 | SAFLINK | Diana Manfredi | T | 5.2.3.2.1 (page 44) | Note that logical access frequently requires specific content within the signature cert (e.g., UPN for Windows logon). If the certs are centrally issued, how will the certs be generated such that use in various logical access environments will be possible using these certs? Is that up to the agency? If so, how is interoperability assured? | None. |
| 60 | SAFLINK | Diana Manfredi | T | 5.2.5 (page 48) | 3rd bullet from the end: How will card be revoked (see SAFLINK comment #53 ). | None. |
| 61 | SAFLINK | Diana Manfredi | G | Sec. 6.0; pg. 49; first and second paragraphs | This Section should be expanded to make it clearer that an agency has the discretion to implement other biometric technologies (such as iris and hand geometry) or other formats of biometric identifiers (such as fingerprint templates). In addition to alternative technologies and data formats, other authentication mechanisms should be mentioned in this Section, including store-on-card/match-on-card and mechanisms where the PIV card acts as a pointer to a biometric data base in a store-off-card/match-off-card approach. | Add the following to the end of second paragraph: "This standard does not restrict the agencies from implementing alternative biometric technologies and data formats."<br><br>Include examples of mechanisms in this Section that illustrate:<br>a) store-on-card/match-on-card<br>b) store-off-card/match-off-card |

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

| Cmt # | Organization | Point of Contact | Comment Type (G-General, E-Editorial, T-Technical) | Section,Annex,etc and Page Nbr | Comment(Include rationale for comment) | Proposed change |
|---|---|---|---|---|---|---|
| 62 | SAFLINK | Diana Manfredi | G | 6.1 (all) | This section is incomplete. Use of the card as an index into a local biometric database for server-based biometric matching should also be included. | Add if appropriate. |
| 63 | SAFLINK | Diana Manfredi | T | Sec. 6.1; pg. 49; 2nd para | For applications that require rapid authentication using biometrics, (e.g. physical access control) agencies should be permitted to store biometrics on the contactless side of the PIV card. The contactless cards have a higher data transfer rate and provide more efficient human factors for rapid authentication. We believe that the use of contact cards for physical access control applications may not be practical due to limitations on card and reader durability in high volume situations and because of environmental considerations (e.g., dust and humidity). We believe that biometric data privacy can be achieved through available contactless technologies (e.g. DESFire triple DES encryption). | Delete the last sentence in this paragraph. |
| 64 | SAFLINK | Diana Manfredi | T | 6.1.2, 2nd para, last sentence (page 51) | Add to the end of the last sentence ", except in combination with other mechanisms (e.g., PIN, biometrics, etc.)." | Change as indicated. |
| 65 | SAFLINK | Diana Manfredi | T | 6.1.3 2nd para (page 52) | 1st sentence reads "The PIV card hosts a signed biometric that can be read from the card after the cardholder provides a PIN to perform CTC authentication." This implies that the biometric container is PIN protected; however, this is not stated in the protection of biometrics section (4.4.6). This is not felt to be necessary, but if retained then external authentication or mutual authentication access controls should be included as acceptable methods rather than just a PIN. | Delete this sentence. |
| 66 | SAFLINK | Diana Manfredi | T | 6.1.3, bullet 1) (page 52) | Incorrect use of term "activating". Replace with "opening". | Change to read "The cardholder is prompted to submit a PIN, **opening** the PIV card ..." |
| 67 | SAFLINK | Diana Manfredi | T | 6.1.3, bullet 1) (page 52) | Requirement for PIN entry greatly reduces the convenience benefit of using a biometric. The most important thing is that the biometric is signed such that its integrity is not questionable. | Delete PIN requirement for biometric container access. |
| 68 | SAFLINK | Diana Manfredi | T | 6.1.5, bullet 2) (page 53) | Incorrect use of term "activating". Replace with "opening". | Change to read "...and the card is **opened**." |

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

| Cmt # | Organization | Point of Contact | Comment Type (G-General, E-Editorial, T-Technical) | Section,Annex,etc and Page Nbr | Comment(Include rationale for comment) | Proposed change |
|---|---|---|---|---|---|---|
| 69 | SAFLINK | Diana Manfredi | T | 6.1.5, para 2) (page 53) | This requirement implies biometric match-on-card. If this is the intent, it should be explicitly stated. | Add if appropriate. |
| 70 | SAFLINK | Diana Manfredi | T | 6.2.1, last para, 2nd sentence (page 54) | States that "Another implication of this standalone environment is that it is infeasible to implement online key management mechanisms for establishing authentication keys between the PIV and the secure site." This is true; however, other means exist for key loading (as well as key diversification schemes). It may be useful to mention these. | Add if appropriate. |
| 71 | SAFLINK | Diana Manfredi | T | Table 6-1, next to last row (Biometric Authentication), 2nd column (page 56). | There are other ways to protect the biometric container (e.g., keys) besides a PIN. Requirement for PIN entry greatly reduces the convenience benefit of using a biometric. If retained, non-PIN options should be identified. | Add if appropriate. |
| 72 | SAFLINK | Diana Manfredi | T | Table 6-1, last row (PACS High Assurance Profile) (page 56). | Biometric authentication should be added as a cardholder authentication method (this would be consistent with 800-63). | Change 2nd entry in 2nd column to read "A PIN **or biometric** is collected from the cardholder." |
| 73 | SAFLINK | Diana Manfredi | T | Annex F: References | Global Platform version 2.0.1 has been superceded by version 2.1.1. | [GP] Global Platform, Card Specification, version 2.1.1, March 2003 |

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical