

## ADMINISTRATIVE LAW DIVISION

\$6.80

## QUESTIONNAIRE

*(Please include a copy of this form with each filing of your rule: Notice of Public Hearing or Comment Period; Proposed Rule, and if needed, Emergency and Modified Rule.)*

DATE: JULY 31, 1998

TO: LEGISLATIVE RULE-MAKING REVIEW COMMITTEE

FROM: (Agency Name, Address & Phone No.) SECRETARY OF STATE

BLDG. 1, SUITE 157-K

CHARLESTON, WV 25305

LEGISLATIVE RULE TITLE: USE OF ELECTRONIC SIGNATURES BY STATE AGENCIES

1. Authorizing statute(s) citation W.VA. CODE §39-5-4

2. a. Date filed in State Register with Notice of Hearing or Public Comment Period:

JULY 1, 1998

b. What other notice, including advertising, did you give of the hearing?

MEMBERS OF INTERGOVERNMENTAL TECHNOLOGY COUNCIL, CONSISTING OF  
REPRESENTATIVES OF EACH STATE OFFICE OR AGENCY.

c. Date of Public Hearing(s) *or* Public Comment Period ended:

JULY 31, 1998

d. Attach list of persons who appeared at hearing, comments received, amendments, reasons for amendments.

Attached X No comments received

- e. Date you filed in State Register the agency approved proposed Legislative Rule following public hearing: (be exact)

**JULY 31, 1998**

---

- f. **Name, title, address and phone/fax/e-mail numbers** of agency person(s) to receive all *written correspondence* regarding this rule: (Please type)

**MARY RATLIFF**

**PHONE: 558-6000**

---

**SECRETARY OF STATE**

**FAX: 558-0900**

---

**BLDG. 1, SUITE 157-K**

**E-MAIL: MRATLIFF@SECRETARY.STATE.WV.US**

---

**CHARLESTON, WV 25305**

---

- g. **IF DIFFERENT FROM ITEM 'f'**, please give **Name, title, address and phone number(s)** of agency person(s) who wrote and/or has responsibility for the contents of this rule: (Please type)

**SAME**

---

---

---

---

3. If the statute under which you promulgated the submitted rules requires certain findings and determinations to be made as a condition precedent to their promulgation:

- a. Give the date upon which you filed in the State Register a notice of the time and place of a hearing for the taking of evidence and a general description of the issues to be decided.

**N/A**

---

---

---

---

b. Date of hearing or comment period:

N/A

c. On what date did you file in the State Register the findings and determinations required together with the reasons therefor?

N/A

d. Attach findings and determinations and reasons:

Attached N/A



## State of West Virginia

Office of the State Auditor  
Building 1, Room W-100  
Charleston, West Virginia 25305

Glen B. Gainer III  
State Auditor

Telephone: (304) 558-2251  
FAX: (304) 558-5200  
Internet: <http://www.wvauditor.com>

August 3, 1998

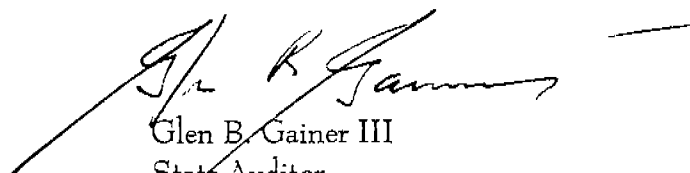
The Honorable Ken Hechler  
Secretary of State  
Building 1, Room 157K  
Charleston, WV 25305

Dear Mr. Hechler:

This letter is to memorialize my approval of the filing of Rules 153-30 and 153-31. I give my approval, however, with reservation to approach the Legislative Rule Making Review Committee should any matters relating to this rule come to my attention after my approval has been given. I take this step because these rules cover matters of national importance and are of great consequence to our state. We must endeavor to incorporate the views of citizens, experts, vendors and others affected thereby.

Thank you for your assistance and direction in this matter. If you have any questions regarding this or any other matters, please do not hesitate to contact me at the above-referenced address.

Sincerely,



Glen B. Gainer III  
State Auditor

GBGIII/lq

## **Statement of Purpose**

§

The purpose of this rule is to allow state, county and municipal agencies to use electronic signature technology with sound security controls to replace manual signatures on documents. This technology will encourage electronic transactions within and among agencies and between the general public and governmental agencies and reduce cost and delays. The rule establishes procedures, notice and security requirements for agencies desiring to accept various types of electronic signatures. It also provides for the method for selection of a uniform digitized signature application to prevent the acquisition of incompatible software by different agencies.

### **Statement of Circumstances**

Efficient governmental action is essential to a strong economy and effective service to citizens. Electronic signatures, with proper security controls, can allow for electronic commerce, speed interactions between agencies, reduce expensive paper transfers of information, and improve service to citizens. Procedures for agencies to identify appropriate transactions for electronic filing, give notice to citizens, and implement the necessary security controls will allow this technology to be implemented effectively.

# APPENDIX B

## FISCAL NOTE FOR PROPOSED RULES

Rule Title: USE OF ELECTRONIC SIGNATURES BY STATE AGENCIES

Type of Rule: X Legislative      Interpretive      Procedural

Agency SECRETARY OF STATE/AUDITOR

Address BLDG. 1, ROOM 157-K

CHARLESTON, WV 25305

### 1. Effect of Proposed Rule

	ANNUAL FISCAL YEAR				
	INCREASE	DECREASE	CURRENT	NEXT	HEREAFTER
<u>ESTIMATED TOTAL COST</u>	\$ 0	\$ 0	\$ 0	\$ 0	\$ 0
PERSONAL SERVICES					
CURRENT EXPENSE					
REPAIRS & ALTERATIONS					
EQUIPMENT					
OTHER					

### 2. Explanation of above estimates:

The use of electronic signatures is anticipated to result in savings at least as great as any costs of programming of software and should not result in overall budgetary changes.

### 3. Objectives of these rules:

Objectives include: elimination of paper generating processes, reduction of time and processing expense, and maintenance of high security fo transactions



Rule Title: USE OF ELECTRONIC SIGNATURES BY STATE AGENCIES

4. Explanation of Overall Economic Impact of Proposed Rule.

A. Economic Impact on State Government.

Long term savings from increased efficiency.

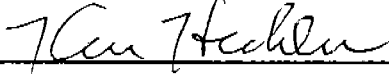
B. Economic Impact on Political Subdivisions; Specific Industries; Specific groups of Citizens.

Beneficial economic impact resulting from enhanced business climate.

C. Economic Impact on Citizens/Public at Large.

Date: June 30, 1998

Signature of Agency Head or Authorized Representative



**TITLE 153**  
**LEGISLATIVE RULES**  
**JOINT RULE OF THE SECRETARY OF STATE AND STATE AUDITOR**

RECEIVED

98 AUG -3 PM 1:44

OFFICE OF THE SECRETARY OF STATE  
STATE OF WEST VIRGINIA

**SERIES 30**

**Use of Electronic Signatures by State Agencies**

**§153-30-1. General**

1.1. Scope. -- This legislative rule establishes the requirements for state agencies intending to use or accept electronic signatures on filings and other messages in electronic form which require the signature of an authorized person.

1.2. Authority. -- W. Va. Code §§ 39-5-4.

1.3. Filing Date. --

1.4. Effective Date. --

**§153-30-2. Definitions**

2.1. "Agency" includes any state, county or municipal office, department, division, bureau, board, commission, public corporation or other governmental entity created by the State Constitution, statute, rule or executive order.

2.2. "Authorized officer" means the elected or appointed official, or a designee, who has authority to act on behalf of the agency.

2.3. "Electronic signature" means any identifier or authentication technique attached to or logically associated with an electronic record that is intended by the person using it to have the same force and effect as a manual

signature. Electronic signatures include, but are not limited to:

2.3.a. A "digitized signature" which consists of a handwritten signature entered on a recording device utilizing electronic recording software which simultaneously converts the image created to a digital record and attaches it to the electronic document to which it relates;

2.3.b. A "digital mark" which consists of an electronic code indicating approval or confirmation which is entered into a protected digital record following access protocols which identify the user and require a password, personal identification number, encrypted card or other security device which restricts access to one or more authorized individuals; and

2.3.c. A "digital signature" which consists of a message transformed using an asymmetric cryptosystem so that a person having the initial message and the signer's public key can accurately determine whether the message was created using the corresponding private key, and whether the message has been altered since the message was transformed.

2.4. "Accept an electronic signature" means to accept an electronic record which requires the signature of an authorized person when that electronic record contains an

electronic signature in lieu of an original signature.

2.5. "Electronic" means electrical, digital, magnetic, optical, electromagnetic, or any other technology that is similar to these technologies.

2.6. "Electronic record" means a record generated, communicated, received, or stored by electronic means.

2.7. "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form, which includes an official record, including but not limited to a message, document, form, return or other instrument which is transmitted electronically from an authorized officer or other person to an agency to meet the requirements of law or to execute an essential transaction. An informal communication will not be considered an electronic record for purposes of this rule.

### **§153-30-3. Agency Use of Electronic Records and Electronic Signatures Generally.**

3.1. Each agency shall determine if, and the extent to which, it will send and receive electronic records and electronic signatures to and from other persons and otherwise create, use, store, and rely upon electronic records and electronic signatures.

3.2. In any case where an agency decides to send or receive electronic records, or to accept document filings by electronic records, the agency may, giving due consideration to security, specify:

3.2.a. The manner and format in which such electronic records must be created, sent, received, and stored;

3.2.b. If such electronic records must be signed, the type of electronic signature that is required or acceptable, the manner and format in which such signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by the sender of the electronic record to facilitate the process;

3.2.c. Control processes and procedures as appropriate to ensure adequate integrity, security, confidentiality, and auditability of such electronic records; and

3.2.d. Any other required attributes for such electronic records that are currently specified for corresponding paper documents, or reasonably necessary under the circumstances.

3.3. Whenever any rule of law requires or authorizes the filing of any information, notice, lien, or other document or record with any agency, a filing made by an electronic record shall have the same force and effect as a filing made on paper in all cases where the agency has authorized or agreed to such electronic filing and the filing is made in accordance with applicable rules or agreement.

3.4. Subject to prior notice by the receiving agency, submission of an electronic record containing an electronic signature record constitutes an agreement by the sender to accept equivalent electronic signature types on return or corresponding electronic records related thereto.

**§153-30-4. Agency Procedures for Adoption, Modification or Revocation of Electronic Signature Acceptance**

4.1. Each agency shall evaluate the types of records received to determine which records can be accepted with electronic signatures, and which form of electronic signature meets the security requirements of the specific transaction.

4.1.a. An electronic record which requires the signature of a person under oath before an authorized official or with the acknowledgment of a notary public may not be accepted with an electronic signature prior to the authorization in law of an electronic attestation.

4.1.b. An electronic record which requires the signature of a person under a self-executing oath may be accepted with a digital signature or other electronic signature which is encrypted, capable of verifying the identity of the signer and discerning any alteration of the message since transformation.

4.2. An agency may accept an electronic record containing an electronic signature only after complying with the procedural requirements of this rule.

4.3. For each type of electronic record on which an agency is willing to accept an electronic signature in satisfaction of a legal signature requirement, the agency shall publish a notice which shall specify:

4.3.a. the name of the agency authorizing use of the electronic record;

4.3.b. a description of the type of electronic record;

4.3.c. the type or types of electronic signature which will be accepted on the record;

4.3.d. a description of any restrictions on who may electronically sign the record;

4.3.e. the date that the electronic record with an electronic signature will first be accepted;

4.3.f. specifications for any procedures or technology that must be used to create, communicate, or store the electronic signature; and

4.3.g. the name of one or more contacts within the agency who can provide additional information, along with the address, telephone and/or e-mail address of the contact person.

4.4. An agency subject to the Administrative Procedures Act, West Virginia Code Chapter 29A-1-1 et seq., shall comply with the notice requirements of section 4.3 prior to acceptance of electronic signatures on electronic records, as follows:

4.4.a. When an agency intends to accept electronic signatures on electronic records sent to or received from employees within the agency or within the department of which the agency is a subdivision, the authorized officer shall give notice as required by section 4.3 to the appropriate personnel.

4.4.b. When an agency intends to accept electronic signatures on electronic records received from other agencies outside the receiving agency's department, the agency shall give notice as required by section 4.3, at least thirty (30) days before first acceptance, to the Information Services and Communications Division of the Department of Administration (IS&C). The IS&C shall

maintain a database of the agencies and the specific information provided for each type of record.

4.4.c. When an agency intends to use or accept electronic signatures on electronic records received from a person acting on his or her own behalf, or from a person acting on behalf of an entity not subject to the Administrative Procedures Act, the agency shall give notice as required by section 4.3, at least thirty (30) days prior to first acceptance, by publication in the State Register.

4.4.d. The agency shall make available a summary of technical or procedural information to assist persons desiring to file electronically and utilize electronic signatures.

4.5. An agency not subject to the Administrative Procedures Act, including county and municipal agencies, shall comply with the notice requirements of section 4.3 prior to its use or acceptance of electronic signatures on electronic records as follows:

4.5.a. When an agency intends to use or accept electronic signatures on electronic records received from employees within the agency or within the governmental entity of which the agency is a subdivision, the authorized officer shall give notice as required by section 4.3 to the appropriate personnel.

4.5.b. When an agency intends to use or accept electronic signatures on electronic records received from a person acting on his or her own behalf, or from a person acting on behalf of an entity other than the governmental entity of which the agency is a subdivision, the agency shall give notice as

required by section 4.3, at least thirty (30) days prior to first acceptance, by publication as a Class I legal advertisement in a qualified newspaper published in the municipality or county where the principal office of the agency is located.

4.6. An agency may modify, suspend, or terminate the acceptance of the electronic signatures following the same procedures as required in this section for adoption, provided, that:

4.6.a. Notice must be given as required at least on hundred twenty (120) days prior to the termination of acceptance of a type of electronic signature; and

4.6.b. In an emergency which prevents the acceptance of the electronic signature, an agency may suspend acceptance of electronic signatures and require filings and signatures be provided on paper. Reasonable notice shall be provided.

4.7. Nothing in this rule shall be construed to require an agency to accept electronic signatures in lieu of written signatures.

4.8. Nothing in this rule shall be construed to allow an agency, without the specific authority of statute, to require a person acting on his or her own behalf, or a person acting on behalf of an entity other than a governmental entity to use an electronic signature in order to complete an essential filing.

4.9. All agencies shall have authority to enter into agreements with other agencies relating to the use and acceptance of

electronic signatures on electronic records communicated between those agencies.

**§153-30-5. Requirements for Acceptance of Digital Marks**

5.1. An agency which intends to accept digital marks shall establish, at a minimum, the security measures and procedural requirements as provided in this section.

5.2. The agency shall establish a secure registry of persons authorized to sign filings and records, or shall utilize a secure registry for verification of the identity of the signer.

5.2.a. A person who desires to become authorized to file with the agency using a digital mark shall file with the secure registry a signed statement verifying that he or she:

5.2.a.1. Will not share with any other person the password, code or other security key required for use of the mark;

5.2.a.2. Agrees that the use of the mark represents confirmation of a record;

5.2.a.3. Agrees to notify the agency immediately once he or she becomes aware that the security key is compromised; and

5.2.a.4. Understands that the provisions of West Virginia Code §61-3C-10 prescribes the penalties for the unauthorized disclosure of a password, identifying code, personal identification number or other confidential security information.

5.2.b. An authorized person shall be issued an identifying number which shall be entered into the registry, along with the date of authorization.

5.2.c. The appropriate administrator shall revoke the access privileges of the authorized person upon termination of authority.

5.3. Each authorized person shall utilize a unique number, password or other personal authorization which shall be encrypted and which shall indicate the approval of the person.

5.4. The size, frequency of required changes and other elements of the security code shall meet state or agency security policies, if any are in effect. If no policy has been adopted, the elements of the security code shall meet generally acceptable standards for password security.

5.5 The agency shall establish the necessary computer hardware and software security, consistent with current generally acceptable standards for secure transactions, to prevent alteration of the electronic filing and to assure protection of the security key, and shall document those features and measures in place.

5.5.a. Information resources shall be protected by use of access control systems. Access control systems can be either internal (passwords, encryption, access control lists, constrained user interfaces) or external (port protection devices, firewalls, host-based authentication).

5.5.b. Rules for access to resources (including internal and external telecommunications and networks) shall be established by the information/application owner or manager who is responsible for the resources.

5.5.c. When confidential or sensitive information from one agency is received by another agency in connection with the transaction of official business, the receiving agency shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing agency.

5.5.d. Pursuant to state security policy, information security and audit controls shall be incorporated into new systems.

5.5.e. Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited, and that violators will be subject to criminal prosecution.

5.6. For filings involving financial transmissions or financial liability, an agency may establish dollar limitations on the amount of a transaction for which a digital mark will be accepted.

#### **§153-30-6. Requirements for Acceptance of Digitized Signatures**

6.1. In order to assure the ease of use of digitized signatures between agencies, and between other persons and agencies, the state shall adopt a uniform system for digitized signature acceptance using software which meets interoperability standards, as defined by

the Information Services & Communications Division of the Department of Administration.

6.2. The Information Services & Communications Division shall initiate a procurement process to identify and obtain the appropriate software. User agencies shall be responsible for the costs of software.

6.3. The agency shall establish security procedures as provided in subsection 5.5. of this rule.

#### **§153-30-7. Requirements for Acceptance of Digital Signatures**

7.1. The Secretary of State, pursuant to legislative rule as required by West Virginia Code §39-5-4, shall establish a certification authority for the registration and issuance of certificates to subscribers for the use of digital signatures, as provided in CSR 153-31.

7.2. An agency which agrees to accept a digital signature in connection with an electronic filing shall obtain, install and test the essential software prior to giving notice of the intent to accept digital signatures.

7.3. Any authorized officer or other authorized person who becomes a subscriber to the certification authority maintained by the Secretary of State and who maintains an authorized key pair shall be permitted to use a digital signature on any electronic document which the agency agrees to accept.

#### **§153-30-8. Requirements for Acceptance of Other Forms of Electronic Signatures**

8.1. When an agency desires to accept a newly developed form of electronic signature

not specifically listed in the definition of electronic signature contained in this rule, the agency shall apply to the Secretary of State for authority to accept the electronic signature.

8.2. To be acceptable as an electronic signature, the technology shall:

8.2.1. Allow the receiving agency to verify the identity of the sender.

8.2.2. Allow the receiving agency to determine whether the message received has been altered en route.

8.3. The agency shall be responsible for assuring the security of the record following its acceptance.



**TITLE 153**  
**LEGISLATIVE RULES**  
**JOINT RULE OF THE SECRETARY OF STATE AND STATE AUDITOR**

**SERIES 30**  
**Use of Electronic Signatures by State Agencies**

**§153-30-1. General**

1.1. Scope. -- This legislative rule establishes the requirements for state agencies intending to use or accept electronic signatures on filings and other messages in electronic form which require the signature of an authorized person.

1.2. Authority. -- W. Va. Code §§ 39-5-4.

1.3. Filing Date. --

1.4. Effective Date. --

**§153-30-2. Definitions**

2.1. "Agency" includes any state, county or municipal office, department, division, bureau, board, commission, public corporation or other governmental entity created by the State Constitution, statute, rule or executive order.

2.2. "Authorized officer" means the elected or appointed official, or a designee, who has authority to act on behalf of the agency.

2.3. "Electronic signature" means any identifier or authentication technique attached to or logically associated with an electronic record that is intended by the person using it to have the same force and effect as a manual

signature. Electronic signatures include, but are not limited to:

2.3.a. A "digitized signature" which consists of a handwritten signature entered on a recording device utilizing electronic recording software which simultaneously converts the image created to a digital record and attaches it to the electronic document to which it relates;

2.3.b. A "digital mark" which consists of an electronic code indicating approval or confirmation which is entered into a protected digital record following access protocols which identify the user and require a password, personal identification number, encrypted card or other security device which restricts access to one or more authorized individuals; and

2.3.c. A "digital signature" which consists of a message transformed using an asymmetric crypto-system so that a person having the initial message and the signer's public key can accurately determine (A) whether the message was created using the corresponding private key, and (B) whether the message has been altered since the message was transformed.

2.4. "Electronic filing" means an official record, including but not limited to a message, document, form, return or other instrument which is transmitted electronically

from an authorized officer or other person to an agency to meet the requirements of law or to execute an essential transaction. An informal communication will not be considered an electronic filing for purposes of this rule.

2.5. "Accept an electronic signature" means to accept an filing— electronic record<sup>1</sup> which requires the signature of an authorized person when that filing— electronic record contains an electronic signature in lieu of an original signature.

2.6 "Electronic" means electrical, digital, magnetic, optical, electromagnetic, or any other technology that is similar to these technologies.<sup>2</sup>

2.7 "Electronic record" means a record generated, communicated, received, or stored by electronic means.<sup>3</sup>

2.8 "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.<sup>4</sup>

<sup>1</sup> Section 39-5-4(a) of the statute authorizes governmental entities to accept electronic signatures on "messages or filings", neither of which is a defined term. Accordingly, wherever these rules refer to "filings," they have been modified to refer to "electronic records" since that term appears to cover both "messages and filings" so as to be consistent with the statute. Presumably, filings and messages are a subset of messages records, and thus, the broader term should also be included (although this relationship is not necessarily clear from the statute).

<sup>2</sup> This definition is taken from the statute at Section 39-5-2(c).

<sup>3</sup> This definition is taken from the statute at Section 39-5-2(d).

<sup>4</sup> This definition is taken from the statute at Section 39-5-2(f).

## §153-30-2A. Agency Use of Electronic Records and Electronic Signatures Generally.<sup>5</sup>

2A.1 Each agency shall determine if, and the extent to which, it will send and receive electronic records and electronic signatures to and from other persons and otherwise create, use, store, and rely upon electronic records and electronic signatures.

2A.2 In any case where an agency decides to send or receive electronic records, or to accept document filings by electronic records, the agency may, by appropriate agency rule, giving due consideration to security, specify:

2A.2.a the manner and format in which such electronic records must be created, sent, received, and stored;

2A.2.b if such electronic records must be signed, the type of electronic signature that is required or acceptable, the manner and format in which such signature must be affixed to the electronic record, and the identity of, or criteria that must be met by any third party used by the sender of the electronic record to facilitate the process;

2A.2.c control processes and procedures as appropriate to ensure adequate integrity, security, confidentiality, and auditability of such electronic records; and

<sup>5</sup> Section 39-5-4(a) of the statute requires the Secretary of State and State Auditor to propose rules to facilitate the use of "electronic signatures." It says nothing about rules relating to the use of electronic records, although those two issues appear to go hand in hand. Accordingly, this new section is proposed as a general overview section that covers both the use of electronic records and the use of electronic signatures.

2A.2.dany other required attributes for such electronic records that are currently specified for corresponding paper documents, or reasonably necessary under the circumstances.

2A.3 Whenever any rule of law requires or authorizes the filing of any information, notice, lien, or other document or record with any agency, a filing made by an electronic record shall have the same force and effect as a filing made on paper in all cases where the agency has authorized or agreed to such electronic filing and the filing is made in accordance with applicable rules or agreement.

2A.4 To the extent reasonable under the circumstances, rules adopted by any agency relating to the use of electronic records or electronic signatures shall be drafted in a manner designed to encourage and promote consistency and interoperability with similar requirements adopted by government agencies of other states and the federal government.

2A.5 In all cases, the act of communicating an electronic record to an agency with the type of electronic signature specified by the agency for that type of electronic record constitutes an agreement by the sender to accept equivalent electronic signature types on return or corresponding electronic records related thereto.<sup>6</sup>

<sup>6</sup> A provision of this type requires more discussion and may be somewhat controversial. However, it is intended to address the problem that appears to be created by statute section 39-5-6(b), which appears to authorize the receiving party to determine the types of electronic signatures that will be accepted by it. It resolves this problem simply by providing that if a party uses a certain type of electronic signature on a communication with a government agency, it is deemed to have agreed to accept an equivalent type of signature

2A.56 Nothing in this Act shall be construed to require any agency to use or to permit the use of electronic records or electronic signatures.

### **§153-30-3. Agency Procedures for Adoption, Modification or Revocation of Electronic Signature Acceptance**

3.1. Each agency shall evaluate the types of electronic filings records it anticipates using or accepting received to determine which electronic records filings can be used or accepted with electronic signatures, and which form of electronic signature meets the security requirements of the specific transaction.

3.1.a. An electronic record filing which requires the signature of a person under oath before an authorized official or with the acknowledgment of a notary public may not be accepted with an electronic signature prior to the authorization in law of an electronic attestation.

3.1.b. An electronic recordfiling which requires the signature of a person under a self-executing oath may be accepted with an electronic signature [only if a digital signature is used.<sup>7</sup>]

on any return communication or other communications relating to the same subject matter.

<sup>7</sup> The issue here is security, not whether the signature used is a digital signature. That is, where a document requires the signature of a person under a self-executing oath, the State is presumably requiring a higher level of attestation by the signer, and increased penalties for false or fraudulent representations. Accomplishing this goal electronically does not necessarily follow as a function of the type of signature used. Rather, it would seem to require something within the document to ensure that the signer understands the seriousness of the statement being made, as well as a somewhat higher

3.2. An agency may accept an electronic record ~~a filing~~ containing an a digital signature, digital mark, digitized signature or other electronic signature only after complying with the procedural requirements of this rule.

3.3. For each type of electronic record on which an agency is willing to accept an electronic signature in satisfaction of a legal signature requirement, the agency shall publish a notice which shall specify: (1) the name of the agency authorizing use of the electronic record, (2) a description of the type of electronic record, (3) the type or types of electronic signature which will be accepted on such record, (4) a description of any restrictions on who may electronically sign such record, (5) the date that such electronic record with an electronic signature will first be accepted, (6) specifications for any procedures or technology that must be used to create, communicate, or store such electronic signature, and (7) the name of one or more contacts within the agency who can provide additional information, along with the

degree of security with respect to the signature in order that the receiving agency can determine with a relatively high degree of certainty that the signature was made by a particular person and, perhaps, that the integrity of the document is intact. These attributes can be satisfied by a digital signature, but not all implementations of a digital signature will satisfy them. Moreover, there may be other technologies that will also satisfy these requirements. Accordingly, a simple requirement for the use of a digital signature seems to present two basic problems. First, it precludes the use of other technologies that may now (or in the future) meet the necessary requirements. Second, it says nothing about how a digital signature must be used and implemented what type of certificate or certification authority must be used, etc. in order to ensure that the digital signature meets the foregoing requirements. Accordingly, this section appears to require a great deal more work and policy analysis before going forward.

address, telephone and/or e-mail address of the contact person.

3.4. An agency subject to the Administrative Procedures Act, West Virginia Code Chapter 29A-1-1 et seq., shall comply with the ~~following~~ notice requirements of section 3.3 prior to its use<sup>8</sup> or acceptance of electronic signatures on electronic records, as follows:

3.4a. When an agency intends to ~~use or~~ accept electronic signatures on electronic records sent to or received from employees within the agency or within the department of which the agency is a subdivision, the authorized officer shall give notice as required by section 3.3 to the ~~[appropriate personnel], of the types of filings and the procedures which will be required.~~

3.4b. When an agency intends to use or accept electronic signatures on electronic records ~~or filings~~ received from other agencies outside the receiving agency's department, the agency shall give notice ~~in writing of its intent~~ as required by section 3.3, at least thirty (30) days before first acceptance, to the Information Services and Communications Division of the Department of Administration (IS&C). The IS&C shall maintain a database of the agencies and the specific information provided for each type of filing.

<sup>8</sup> As originally written, this Section assumes a one-way communication -- i.e., it is concerned with electronic signatures on filings submitted to the agency. It says nothing about electronic signatures on messages sent by the agency to others. Since Section 39-5-4(a) requires the Secretary of State and the state auditor to propose rules "to facilitate the use of electronic signatures" This presumably implies both sending and receiving electronically signed documents.

3.43.c. When an agency intends to use or accept electronic signatures on electronic filings records received from a person acting on his or her own behalf, or from a person acting on behalf of an entity not subject to the Administrative Procedures Act, the agency shall give notice of its intent as requested by section 3.3, at least thirty (30) days prior to first acceptance, by publication in the State Register.

~~3.3.d. For each type of electronic message or filing that an agency is willing to accept, in the notice required in subdivisions 3.3.b. and 3.3.c., the agency shall include give the name of the agency authorizing receiving use of the electronic message or the filing, a description of the type of electronic message or filing, the type or types of electronic signature which will be accepted, a description of any restrictions on who may file, the date that an electronic message or filing with an electronic signature will first be accepted, and the name of one or more contacts within the agency who can provide additional information, along with the address, telephone and/or e-mail address of the contact person.~~

3.43.ed. The agency shall make available a summary of technical or procedural information to assist persons desiring to file electronically and utilize electronic signatures.

3.54. An agency not subject to the Administrative Procedures Act, including county and municipal agencies, shall comply with the following notice requirements of section 3.3 prior to its use or acceptance of electronic signatures on electronic records as follows:

3.54.a. When an agency intends to use or accept electronic signatures on

electronic filings records received from employees within the agency or within the governmental entity of which the agency is a subdivision, the authorized officer shall give notice as required by section 3.3 to the [appropriate personnel.] of the types of filings and the procedures which will be required.

3.54.b. When an agency intends to use or accept electronic signatures on electronic records received from a person acting on his or her own behalf, or from a person acting on behalf of an entity other than the governmental entity of which the agency is a subdivision, the agency shall give notice as required by section 3.3 of its intent, at least thirty (30) days prior to first acceptance, by publication as a Class I legal advertisement in a qualified newspaper published in the municipality or county where the principal office of the agency is located.

~~3.4.e. In the notice, the agency shall give the same information as required in section 3.3.d.~~

3.65 An agency may modify, suspend or terminate the acceptance of the electronic signatures following the same procedures as required in this section for adoption, provided, that:

3.65.a. Except in the case of an emergency caused by the failure of computer hardware, software, or communication systems, Notice must be given as required at least on hundred twenty (120) days prior to the termination of acceptance of a type of electronic signature; and

3.65.b. In an emergency caused by the failure of the computer hardware, software, or communication systems required for the acceptance of the electronic signature, an agency may require filings and signatures

be provided on paper without prior notice [???].

3.76. Nothing in this rule shall be construed to require an agency to accept electronic signatures in lieu of written signatures.

3.87. Nothing in this rule shall be construed to allow an agency, without the specific authority of statute, to require the use of electronic records and electronic signatures in lieu of paper ~~a person acting on his or her own behalf, or a person acting on behalf of an entity other than the governmental entity to use a digital signature in order to complete an essential filing.~~

3.98. All agencies shall have authority to enter into agreements with other agencies relating to the use and acceptance of electronic signatures on electronic ~~records, messages or filings communicated~~ between those agencies.

#### **§153-30-4. Requirements for Acceptance of Digital Marks**

4.1. An agency which intends to accept digital marks shall establish, at a minimum, the security measures and procedural requirements as provided in this section.

4.2. The agency shall establish a secure registry of persons authorized to sign filings and records, or shall utilize a secure registry for verification of the identity of the signer.<sup>2</sup>

<sup>2</sup> This section appears to contemplate two radically different concepts - a registry of persons "authorized" to sign filings versus a registry for "verification of identity" of the signer. I am not sure what is intended here. Also, who maintains this registry, and what are the rules governing their performance? See, for example, the rules in the Series 31 regulations

4.2.a. When an agency maintains its own registry, a person who desires to become authorized to file with the agency using a digital mark shall file a signed statement verifying that he or she:

4.2.a.1. Will not share with any other person the password, code or other security key required for use of the mark;

4.2.a.2. Agrees that the use of the mark represents approval and agreement to the contents of a filing<sup>10</sup>;

4.2.a.3. Agrees to notify the agency immediately if he or she becomes aware that the security key is compromised<sup>11</sup>; and

4.2.a.4. Understands that the provisions of West Virginia Code §61-3C-10

governing the entity maintaining a digital certificate repository.

<sup>10</sup> It cannot be said that the use of a signature always represents "approval and agreements to the contents" of a filing. It may, for example, indicate simply that the information contained in the document has been disclosed to the person signing the document (e.g., a notice function), or that the contents of the document are being provided by the signer (e.g., an indication of source), but without any evidence of approval or agreement to the contents. Accordingly, the terms of this section appear to go much farther than is appropriate for all circumstances.

<sup>11</sup> This section raises a controversial issue with respect to the obligations of an individual (particularly a consumer) to provide notice that a security key, private key, PIN number, or other signature device has been compromised, as well as such person's liability for the unauthorized use of that security device following compromise. As currently written, this section could create an implication that failure to comply with its terms (i.e., to notify the agency immediately upon becoming aware of a compromise) exposes the individual to liability for unauthorized use of the security key.

prescribes the penalties for the unauthorized disclosure of a password, identifying code, personal identification number or other confidential security information.

4.2.b. An authorized person shall be issued an identifying number which shall be entered into the registry, along with the date of authorization.

4.2.c. The appropriate administrator shall revoke the access privileges of the authorized person upon termination of authority.

4.3. Each authorized person shall utilize a unique number, password or other personal authorization which shall be encrypted and which shall indicate the approval of the person.

4.4. The size, frequency of required changes and other elements of the security code shall meet state or agency security policies, if any are in effect. If no policy has been adopted, the elements of the security code shall meet generally acceptable standards<sup>12</sup> for password security.

4.5 The agency shall establish the necessary computer hardware and software security, consistent with current generally acceptable standards for secure transactions, to prevent alteration of the electronic filing and to assure protection of the security key, and shall document those features and measures in place.<sup>13</sup>

---

<sup>12</sup> Do such standards exist?

<sup>13</sup> This provision appears to be generally applicable to all electronic transactions in which the state is involved. Perhaps it should be moved in order to make this clear.

4.5.a. Information resources shall be protected by use of access control systems. Access control systems can be either internal (passwords, encryption, access control lists, constrained user interfaces) or external (port protection devices, firewalls, host-based authentication).<sup>14</sup>

4.5.b. Rules for access to resources (including internal and external telecommunications and networks) shall be established by the information/application owner or manager who is responsible for the resources.<sup>15</sup>

4.5.c. When confidential or sensitive information from one agency is received by another agency in connection with the transaction of official business, the receiving agency shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing agency.<sup>16</sup>

---

<sup>14</sup> This provision appears to be generally applicable to all electronic transactions in which the state is involved. Perhaps it should be moved to reflect this.

<sup>15</sup> This section also appears to be generally applicable.

<sup>16</sup> This Section governs the confidentiality of sensitive information sent from one government agency to another. While this is an important issue, it seems like an inappropriate subject for these rules governing the use and acceptance of electronic records and electronic signatures -- i.e., I presume that the obligation of the receiving agency to keep sensitive information confidential applies equally to paper as to electronic records. The only issue, it would appear, is what procedures must be put in place to keep electronic records (as opposed to paper records) secure and confidential. While the procedures may differ between paper and electronic records, it may not be necessary for those issues to be addressed in these rules. Alternatively, such issues relating to confidentiality of sensitive information are generally applicable to all electronic communications in which the state is involved, and should not be limited to electronic communications involving digital marks.

4.5.d. Information security and audit controls shall be incorporated into new systems.<sup>17</sup>

4.5.e. Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited, and that violators will be subject to criminal prosecution.<sup>18</sup>

4.6. For filings involving financial transmissions or financial liability, an agency may establish dollar limitations on the amount of a transaction for which a digital mark will be accepted.

#### **§153-30-5. Requirements for Acceptance of Digitized Signatures**

5.1. In order to assure the ease of use of digitized signatures between agencies, and between other persons and agencies, the state shall adopt a uniform system for digitized signature acceptance using a single software provider.<sup>19</sup>

---

<sup>17</sup> This section is also generally applicable to all state electronic communications. Moreover, the provision is so general and broad as to appear to be of little value.

<sup>18</sup> This provision also appears to be one of general applicability.

<sup>19</sup> The need to adopt a uniform system for digitized signature acceptance using a single software provider appears to be relevant only for those instances in which something more than a digitized image of a signature is required -- e.g., applications wherein a digitized signature is automatically compared to a database of digitized signatures or signature dynamics elements for verification of identity purposes, or applications wherein the digitized signature is linked to the message in a manner such that if the message or signature is altered the signature will be invalidated. There are, however, presumably numerous situations wherein digitized signatures would be an acceptable substitute for a handwritten signature, but which do not otherwise

5.2. The Information Services & Communications Division of the Department of Administration shall initiate a procurement process to identify and obtain the appropriate software.

5.3. The agency shall establish security procedures as provided in subsection 4.5. of this rule.

#### **§153-30-6. Requirements for Acceptance of Digital Signatures<sup>20</sup>**

6.1. The Secretary of State, pursuant to legislative rule as required by West Virginia Code §39-5-4, shall establish a certification authority for the registration and issuance of

---

require the higher level of security afforded by the foregoing examples. For example, there are presumably numerous state transactions (such as applying for a fishing or hunting license) where a signature is required but there is normally no need for further verification of identity. In such cases, presumably any system that would attach a digitized signature is sufficient. Or putting it another way, requiring a single unified digitized signature software product assumes a level of security that may not be required in all cases.

Requiring a single source of digitized signature software also, presumably, requires persons signing such electronic records to make an investment in the software at their end, which presumably makes it much more difficult for the state to change digitized system software products subsequently.

<sup>20</sup> This section ignores numerous issues that should be addressed before the state is going to accept digital signatures. Addressing those issues requires a fundamental determination as to whether the intent of the section is only to accept digitally signed documents that can be verified by a certificate issued by the state certification authority, or whether the state is willing to accept digitally signed documents verified by certificates issued by private certification authorities so long as they meet certain requirements or are otherwise authorized or certified by the state.



certificates to subscribers for the use of digital signatures.<sup>21</sup>

6.2. An agency which agrees to accept a digital signature in connection with an electronic filing shall obtain, install and test the essential software prior to giving notice of the intent to accept digital signatures.

6.3. Any person who becomes a subscriber to the certification authority maintained by the Secretary of State and who maintains an authorized key pair shall be authorized to use a digital signature on any electronic document which the agency agrees to accept.<sup>22</sup>

#### **§153-30-7. Requirements for Acceptance of Other Forms of Electronic Signatures**

7.1. When an agency desires to accept a newly developed form of electronic signature not specifically listed in the definition of electronic signature contained in this rule, the agency shall apply to the Chief Technology Officer for authority to accept the electronic signature.

7.2. To be acceptable as an electronic signature, the technology shall:

<sup>21</sup> It is not clear as to the intent of this section. Does this rule indicate that the state cannot accept a digital signature unless it can be verified by reference to a certificate issued by the certification authority established by the state? Alternatively, is this section meant to require the establishment of a state certification authority only for purposes of issuing certificates to state employees and state agents to verify signatures they create when communicating to others?

<sup>22</sup> I am not sure that this section is appropriate. Just because I have obtained a certificate from the state Certification Authority does not necessarily mean that I am automatically authorized to sign any electronic document the agency agrees to accept.

7.2.1. Allow the receiving agency to determine the identity of the sender.<sup>23</sup>

7.2.2. Allow the receiving agency to determine whether the message received has been altered en route or is incomplete.<sup>24</sup>

7.2.3. Ensure that the sender cannot falsely deny sending the message nor falsely deny its content.<sup>25</sup>

7.3. The agency shall be responsible for assuring the security of the filing following its acceptance.

<sup>23</sup> Some of the currently existing and authorized forms of electronic signature do not necessarily allow the receiving agency to determine the identity of the sender. For example, a digitized signature may look like an unreadable scribble, and by itself, is not sufficient to determine the identity of the signer. Thus, imposing this requirement on new forms of electronic signatures may not be appropriate. This should be discussed further.

<sup>24</sup> As with the issue raised in the prior footnote, there is no currently existing requirement that acceptable electronic signatures allow the receiving agency to determine whether the message received has been altered in route or is incomplete. The definition of a digital signature does allow the recipient to determine whether the message has been altered, but says nothing about whether the message is incomplete so long as what is received is the same as what was digitally signed. Other forms of electronic signature, such as digitized signatures and digital marks do not, by definition, provide any information regarding alteration or completeness. Thus, it appears inappropriate to impose this requirement on new forms of electronic signature.

<sup>25</sup> As with the prior two footnotes, this requirement does not appear with respect to other forms of electronic signature.