Virginia Regulatory Town Hall
townhall.virginia.gov

Final Regulation
Agency Background Document

Agency name	Library of Virginia (The Library Board)
Virginia Administrative Code (VAC) citation	17 VAC 15-120
Regulation title	Elimination of Social Security Numbers in Public Records
Action title	Regulations Governing the Destruction of Public Records Containing Social Security Numbers
Date this document prepared	July 9, 2008

This information is required for executive branch review and the Virginia Registrar of Regulations, pursuant to the Virginia Administrative Process Act (APA), Executive Orders 36 (2006) and 58 (1999), and the *Virginia Register Form, Style, and Procedure Manual.*

Brief summary

Please provide a brief summary (no more than 2 short paragraphs) of the proposed new regulation, proposed amendments to the existing regulation, or the regulation proposed to be repealed. Alert the reader to all substantive matters or changes. If applicable, generally describe the existing regulation. Also, please include a brief description of changes to the regulation from publication of the proposed regulation to the final regulation.

This new regulation is mandated by the *Code of Virginia* to provide direction on the appropriate destruction of public records containing social security numbers whose retention periods have expired.

Statement of final agency action

Please provide a statement of the final action taken by the agency including (1) the date the action was taken, (2) the name of the agency taking the action, and (3) the title of the regulation.

At its meeting on March 17, 2008 the Library Board approved the promulgation of 17 VAC 15-120, Elimination of Social Security Numbers in Public Records.

.

Legal basis

Please identify the state and/or federal legal authority to promulgate this proposed regulation, including (1) the most relevant law and/or regulation, including Code of Virginia citation and General Assembly chapter numbers, if applicable, and (2) promulgating entity, i.e., agency, board, or person. Describe the legal authority and the extent to which the authority is mandatory or discretionary.

The statutory authority of the Library Board to promulgate this regulation can be found in § 42.1-82.A of the *Code of Virginia*, which states: The State Library Board shall:

1. Issue regulations concerning procedures for the disposal, physical destruction or other disposition of public records containing social security numbers. The procedures shall include all reasonable steps to destroy such documents by (i) shredding, (ii) erasing, or (iii) otherwise modifying the social security numbers in those records to make them unreadable or undecipherable by any means.

Purpose

Please explain the need for the new or amended regulation. Describe the rationale or justification of the proposed regulatory action. Detail the specific reasons it is essential to protect the health, safety or welfare of citizens. Discuss the goals of the proposal and the problems the proposal is intended to solve.

This regulation is mandated to prevent identity theft based on social security numbers found in public records whose retention periods have expired. The regulation provides specific direction on the destruction of this type of record. The purpose of the regulation is to protect individuals from identity theft by eliminating unauthorized access to social security numbers in public records whose retention period has expired.

Substance

Please identify and explain the new substantive provisions, the substantive changes to existing sections, or both where appropriate. A more detailed discussion is required under the "All changes made in this regulatory action" section.

Additional definitions were added for clarity. The size requirement and shredding method were eliminated after discussion from the affected business community as to economic hardship this would cause. Process used by small businesses was deemed effective after process was explained. Extraneous information was removed from regulation.

Issues

Please identify the issues associated with the proposed regulatory action, including:
1) the primary advantages and disadvantages to the public, such as individual private citizens or businesses, of implementing the new or amended provisions;
2) the primary advantages and disadvantages to the agency or the Commonwealth; and
3) other pertinent matters of interest to the regulated community, government officials, and the public.
If there are no disadvantages to the public or the Commonwealth, please indicate.

The primary benefit from this regulation for citizens is the deterrence of identity theft by outlining actions to be taken to remove social security numbers from public records whose retention period has expired. The regulation as currently written reflects input from the affected business community.

There are no advantages associated with this regulation to the Library of Virginia.

There are no known disadvantages associated with this regulation for the public, Commonwealth or the promulgating agency.

Changes made since the proposed stage

Please describe all changes made to the text of the proposed regulation since the publication of the proposed stage. For the Registrar's office, please put an asterisk next to any substantive changes.

Section number	Requirement at proposed stage	What has changed	Rationale for change
120-10	No definitions for backup tapes, custodian, and pulped added to definition of electronic record	Definitions were added Incinerated used in place of burned Format of Section B adjusted and corrected	Clarity
120-20		Purpose of regulation more clearly stated	Clarity
	Phrases "other privacy protected information" and "privacy protected data' used	References eliminated as outside scope of regulation	Clarity
	Timing of overwriting of backup tapes	Phrases referencing of overwriting of backup tapes eliminated and replaced with the requirement that data be totally obliterated	Clarity
	Overwriting of data on floppy disks, tapes or magnetic media	Requirement that data be overwritten multiple times eliminated as excessive and not current practice	Clarity
	Crosscutting and shredding to 3/8 inch or less by contractors	* This requirement written to apply only to shredding done within an agency or office. Statement added that destruction shall be witnessed by an agency representative if performed by a contractor.	Eliminates an overly onerous requirement on the small business community

Public comment

Please summarize all comments received during the public comment period following the publication of the proposed stage, and provide the agency response. If no comment was received, please so indicate.

Commenter	Comment	Agency response
Jerome Kendall	Include "machine-readable" in the definition of electronic record	Did not include
	Include a definition for "media".	Did not include
	In the very last paragraph, reference is made to "or other privacy-protected information" in addition to Social Security numbers. This should be added into the paragraph that begins "Public records, regardless of media" as "that contain social security numbers OR OTHER PRIVACY-PROTECTED INFORMATION must be shredded...."	Deleted reference to other privacy-related matter as beyond scope of regulation
	Social Security" refers to the specific Social Security program, and should therefore be capitalized.	Capitalized Social Security
	Section B, #2: The very idea that IT shops in every political subdivision of the Commonwealth are actually going to time the overwriting/degaussing of privacy-protected information residing on back-up tapes to be simultaneous with the destruction of the privacy-protected information which those tapes actually back-up is almost certainly going to be laughed at by those IT shops. I suggest the language be modified to simply assert that the back-up tapes should be overwritten, wiped, or degaussed to the extent necessary to ensure the irretrievability of the data on them, but that a more reasonable period of time be allowed for; 30 - 60 days, perhaps	Did not include requirement that this action be simultaneous
Jerry Palmer	I am not pleased with the idea of requiring a cross cut shredder. In addition to the expense of purchasing one (I have no budget to do so, what with State budget cuts), I want to mention other problems associated with a large cross cut operation: It's a fine machine for in-office use wherein small amounts of shredding are required. In a major operation such as mine, shredding 25-30 tons yearly, cross cuts pose health and dust problems. VT had one over ten years ago and disposed of it, as operators had to wear masks and the dust and debris were unbearable, not to mention the noise level, requiring ear	This requirement written to apply only to shredding done within an agency or office. Statement added that destruction shall be witnessed by an agency representative if performed by a contractor.

	plugs. My EHHS folks were very pleased we swapped out for a strip shredder. While it's product is more easily reconstructed than the output of a cross cut, I have always felt the job is more than adequate. Let's put it this way: if I wanted a SS#, I can think of 1900 ways easier to acquire it than to try to reconstruct the record from a #60 bale containing approximately 5000 individual strip shredded records. I know there are other state records managers who share my view and are satisifed with strip shredding.	
Karen Linett	Agrees with Mr. Palmer's comment	This requirement written to apply only to shredding done within an agency or office. Statement added that destruction shall be witnessed by an agency representative if performed by a contractor.
Tina Long	SHREDDING: The federal government has approved the following filter screen hole sizes of 3/32, 1/8, or 4 mm as being secure	Did not include
	) Pulped, burned, records custodian, and magnetic erasing are not defined. 2) "Overwritten" is defined, however, I suggest defining "electronic erasing" or "file wiping". 3) "Shredding" contains two definitions - (a) the action, and (b) the type of machine to use. 4) "Electronic record" is defined but maybe just "Records" should be defined so as to include the paper records metioned (Sic) in section 30.	
	1) Purpose, lists various methods of destruction but they are not defined in Section 10 and not offered as an option in Section 30. [purpose means: intent, intention, meaning, mission]	Purpose more clearly stated
	SECTION 30: 1) subsection A contains two different topics - (a) how to destroy paper records, and (b) responsibilities of the records custodian. I suggest separating them. 2) subsection A, second paragraph last sentence states "The agency contracting for the shredding retains responsibility..." Since there is no security, or guarantee, I would change it to read that an employee of the agency shall witness the destruction of materials if done off-site, or through a	

	contractor. 3) subsection B suggests electronic records have a different retention life than paper records. I may be wrong, but most electronic and paper records should have the same retention life, being that one is the same as the other aside from the medium. 4) subdivision 1 of subsection B says files stored on a computer must be deleted and overwritten. However, subdivisions 2 and 3 say back-up tapes, floppy disks, or other magnetic storage devices only have to be overwritten. I may be wrong, but a 'file' can refer to a single document or part of the agencies file scheme (computer). 5) subdivision 5 of subsection B mentions privacy-protected information. Maybe the Title of Chapter 120 should include: ... SECURITY NUMBERS AND PRIVACY-PROTECTED INFORMATION. 6) subdivision 3 of subsection B says that data... on flopy disks, tapes and other... must be overwritten - B.3.a. says disks, tapes and other... must be shredded or exposed to a magnetic field. QUESTION: are they saying the data shall be overwritten and the medium it is on shall be shredded? or are there two different procedures - or something?	
	change the word 'must' to 'shall' and consider spending more time on this chapter.	
John Breeden	Section 17 VAC 15-120-30, B Electronic re Procedure #2 requires that “back-up tapes n overwritten at the same time as all other cop destroyed. Tapes shall be held no longer th conclusion of the retention period for the in contained in the tape.” Procedure B, #5 intr privacy protected information” The first tw relate to Procedure #2 and the third commer Procedure #5 of the regulation.<-xml:names o ns = "urn:schemas-microsoft-com:office:c	
	1. Are back-up tapes considered records or non-records- If they are non-records, does the Library Board have the authority to issue regulations regarding the physical destruction of social security numbers on back-up tapes or does the Virginia Information Technology (VITA) establish back-up tape policies and procedures for	

	state agencies	
	2. Assuming the answer to the first question is that the Library Board has this authority, VITA and local Information Technology departments probably have varying policies and procedures for tape back-up creation and rotation. One typical procedure for many IT groups is to backup Microsoft Exchange and Windows Servers nightly from Monday through Thursday or Friday, retaining those tapes for 30 days. The last tapes of the week, either those created on Friday or Saturday, are retained for 90 days. The last tapes created during the month are typically retained for 12 months. These procedures would result in back-up tapes containing social security numbers being retained for as long as a year after the record might have been destroyed. Would such tape back-up and rotation procedures be in violation of section 17 VAC 1-120-30, B #2 that requires that back-up tapes be "overwritten at the same time"- I recommend changing the requirement to either "30 days" or "60 days	
	3. Section 5 is the first place that "other privacy protected information" is introduced. While think it important to protect other private information, this regulation's title indicates it is for the destruction of social security numbers and "other privacy protected information" a been added here as an afterthought, with the user not provided any information about what constitutes other privacy protected information. I recommend identifying the other private i that requires this stringent regulation, if such requirements are warranted, or limiting the regulation to social security numbers.	Phrase "other privacy-protected information" has been deleted from regulation
Richard Harrington	Although other forms of destruction are mentioned in the first paragraph, it should be clarified that burning can be done for all the media below including CD's as an acceptable form of destruction for records containing SSN's and other "privacy protected information" if this is defined in	"Incinerated" is substituted for "burned" Reference to other privacy protected information is deleted

	the paper. Adding "other privacy protected information" is not appropriate for this regulation unless you change the title and define what is meant by this statement.	
	I concur with Mr. Breeden's comments about if back-up tapes are really considered a "record", and also the other's comments about it is impractical to require that they be erased at the same time as the destruction of the records. Allowing a reasonable time within the destruction time frame seems more appropriate for back-up tapes especially since they may contain other information that is not yet eligible for destruction. This would entail identifying what is eligible for destruction on the tapes from what is not - a difficult and time consuming task on back-ups.	
Virginia A Jones	There are several inconsistencies in this proposed regulation, as well as some requirements that are overly specific. Inconsistencies include: 1. Definition of "shredding." This definition also includes a description of a particular type of shredder (cross-cut) which should be either a part of it's own definition or part of a more descriptive sentence placing it in the context of "shredding." 2. As "electronic shredding" is a viable choice, the term should also be included in the definition to distinguish it from paper or other hard media shredding. For example, Wikipedia defines it as: "In computing, file shredding	

		or file wiping is the act of deleting a computer file securely, so that it cannot be restored by any means. This is done either using file shredder software, or by issuing a "secure delete" command, as opposed to a "delete" command from the operating system." (en.wikipedia.org/wiki/Shredding)	Definitions have been added. Burned replaced by incinerated
		3. The Purpose includes two terms that are not defined – "pulped" and "burned."	Regulation refers only to elimination of Social Security Numbers. Reference to other privacy protected information has been eliminated.
		4. The Purpose states that "Public records… that contain Social Security numbers… ." The Government Data Collection and Dissemination Practices Act (Code of Virginia §2.2-3800 et. seq.) defines other personal information that must also be kept private as well as how Social Security numbers must be safeguarded. While section B5 alludes to protecting this other defined personal information, this proposed regulation does not include its protection in all the requirements. It should. This will also entail revising the title of the proposed	Suggestion incorporated into the regulation.

	regulation. 5. Section A states that paper records must be shredded by cross-cut shredder then states that the shredder must reduce the paper to "strips" no wider than 3/8 inches. This can be confusing. It would be better to say "that reduces the paper to a size no wider than 3/8 inches."	Suggestion incorporated into the regulation.
	6. Section A should include the requirement that an employee shall witness the destruction of materials containing medical information as required by the Health Information Portability and Protection Act (HIPPA) if shredding is done through a contractor or other agency or department.	Distinction made between physical media agency plans to maintain and media it plans to destroy.
	7. Section B3 states data on disks, tapes and other magnetic storage devices must be overwritten, but section B3a states the same media must be shredded or exposed to a powerful magnetic field. One requirement needs to be set. Either eliminate one or the other, or combine them into one.	Multiple overwriting eliminated as a requirement.
	Overly specific requirements includes: 1. Section B1 states that "use of software programs that overwrite the data… multiple times… must be utilized." By context, this requirement is also placed on "back-up tapes, floppy disks, tapes, and other magnetic storage devices"	

		in sections B2 and B3. This simply is not necessary in modern computer systems to provide the level of protection needed for this type of data. NIST 800-88 (Recommendations of the National Institute of Standards and Technology, September, 2006) states that "studies have shown that most of today's media can be effectively cleared by one overwrite." NIST 800-88 also separates file disposal into four categories. Category two "clearing" is defined as: "A level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Simple deletion of items would not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. For example, overwriting is an acceptable method for clearing media. There are overwriting software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations.	

	The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not writeable." This level of disposal is adequate for most state and locality systems containing social security numbers and other defined "personal information." 2. Section B2 places this multiple overwrite requirement on backup tapes unnecessarily. Correctly defining backup tapes in the regulation as "created as redundant datasets used to restore systems only in the case of emergencies, that are overwritten on a regular basis" will suffice. Backup tapes meeting this definition are constantly overwritten as they are rotated through a scheduled backup process. If tapes are used for retention or other purposes, then section B3 would cover them.	Multiple overwriting eliminated as a requirement.

All changes made in this regulatory action

Please detail all changes that are being proposed and the consequences of the proposed changes. Detail new provisions and/or all changes to existing sections.

Current section number	Proposed new section number, if applicable	Current requirement	Proposed change and rationale
17VAC15-120-10			For clarity added definitions of backup tapes. custodian, pulped
17VAC15-120-20			Reworded purpose for clarity Replaced burned with incinerated Capitalized Social Security
17VAC15-120-30			For clarity added "pulped or incinerated." Added "If paper records are destroyed within an office or agency, records shall be

			shredded" Replaced strips with "a size" Added "by another agency or department, or by contractor" Capitalized Social Security Added "A representative of the contracting agency shall witness the destruction." Added "Agencies may maintain or destroy the physical media." Added 'using software that overwrites with meaningless data to totally obliterate the original data to prevent information from being reconstructed." Deleted "to prevent the information from being reconstructed. Software programs that overwrite the data with meaningless data multiple times to totally obliterate the original data must be utilized for overwriting." Added "to totally obliterate the original data." Deleted "at the same time as all other copies are destroyed. Tapes shall be held no longer than the conclusion of the retention period for the information contained in the tape." Deleted "3. Data containing social security numbers on floppy disks, tapes, and other magnetic storage devices must be overwritten. a. Disks, tapes and other magnetic media must be shredded in a shredder to insure that the information is totally destroyed or the materials must be exposed to a powerful magnetic field to disrupt information. b. If the magnetic media are used, the data must be reviewed to insure that the social numbers are not retrievable." 4. Added incinerated 5. Deleted "or other privacy-protected information" and "privacy-protected data" These changes were made for clarity.

Regulatory flexibility analysis

Please describe the agency's analysis of alternative regulatory methods, consistent with health, safety, environmental, and economic welfare, that will accomplish the objectives of applicable law while minimizing the adverse impact on small business. Alternative regulatory methods include, at a minimum: 1) the establishment of less stringent compliance or reporting requirements; 2) the establishment of less stringent schedules or deadlines for compliance or reporting requirements; 3) the consolidation or simplification of compliance or reporting requirements; 4) the establishment of performance standards for small businesses to replace design or operational standards required in the proposed regulation; and 5)

the exemption of small businesses from all or any part of the requirements contained in the proposed regulation.

Based on the discussion with the small business community the requirement that crosscutting and shredding to 3/8 inch or less be used by contractors was eliminated as overly onerous.

Family impact

Please assess the impact of the proposed regulatory action on the institution of the family and family stability including to what extent the regulatory action will: 1) strengthen or erode the authority and rights of parents in the education, nurturing, and supervision of their children; 2) encourage or discourage economic self-sufficiency, self-pride, and the assumption of responsibility for oneself, one's spouse, and one's children and/or elderly parents; 3) strengthen or erode the marital commitment; and 4) increase or decrease disposable family income.

This regulation will help prevent identity theft. It will have no impact beyond that on nurturing or eroding the rights of parents, encouraging economic self-sufficiency, self-pride, assumption of responsible for oneself, one's spouse, and one's children and elderly parents; and strengthen or erode the marital commitment; and increase or decrease disposable family incomes.