Comprehensive Public Comments and SSA Responses for:
Electronic Consent Based Social Security Number Verification

OMB No. 0960-0817

Note: *This document compiles and summarizes public comments on eCBSV from the following sources: 1) written comments submitted to SSA during two public comment periods following publication of the requisite Paperwork Reduction Act (PRA) Federal Register Notices (**Federal Register Notice 1**; **Federal Register Notice 2**); 2) a listening session the Big Tent Coalition (BTC) requested from the Office of Management and Budget, with SSA in attendance, held on April 30, 2021; and 3) two eCBSV discussions between the BTC and SSA, held on April 22, 2021 and May 6, 2021.*

Part I: Comments Relating to the Current Information Collection Request (i.e., New Material for eCBSV Phase II)

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
Comment #1: The BTC objected to restrictions on the "transferring" and "processing" of SSN Verifications or Written Consents, stating these restrictions will harm American consumers abroad who will be transacting business with Permitted Entities (PEs) or Financial Institutions (FIs), such as service members or vacationers. This could even lead to the perpetuation of fraud from outside the jurisdiction of the United States. The BTC similarly objected to the requirement that data be stored within the United States. (*see sections III.A.22 and V.A.5.*)	**Response #1:** SSA is not placing restrictions on the location of the *consumer*. The consumer can be anywhere, and it is the responsibility of the Permitted Entity to ensure all data is encrypted at rest and in transit. Rather, SSA's requirement applies only to where the SSA data is *stored*. Internet and infrastructure, and the processing of requests from consumers overseas, are not in the scope of this requirement. To clarify this policy, SSA agrees to remove the references to "processing" and "transferring" from the relevant section of the User Agreement. However, we will still require Permitted Entities to ensure that data is *stored* within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the U.S. Virgin Islands.	SSA has partially compromised by offering to modify User Agreement language per the BTC's suggestion.	SSA cannot permit SSA data to be stored outside of the United States due to the multitude of foreign laws to which SSA data would be subject if stored outside of the United States. Foreign laws may authorize access to data stored within a certain country that go beyond access, which SSA would permit under the Privacy Act or the Social Security Act.

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
Comment #2: Due to the concerns expressed in comment #1, the commenters asked that we remove all references to "processing" and "transferring" in the proposed new sections of both the User Agreement and Technical Specifications documents.	**Response #2:** As we mentioned above, SSA agrees to remove the references to "processing" and "transferring" from the relevant sections of the User Agreement (the Technical Information Guide is not undergoing PRA approval, but we can make similar changes there).	Issue resolved; SSA agrees to remove the words requested by commenters.	N/A
Comment #3: Changes should be limited in scope to "SSN Verifications" only, not "Written Consents." The scope of the proposed changes in both the User Agreement and Technical Specifications should be limited in applicability solely to SSN Verifications. References to Written Consent in the proposed new sections should be deleted.	**Response #3:** SSA agrees to remove the phrase "Written Consent" from the following provisions regarding cloud service providers and managed service providers that were added to the eCBSV User Agreement as part of the most recent PRA filing: III.A.22, V.A.5. However, in response to fuller comments made by public commenters on this issue, we would like to clarify two points. First, regardless of who "owns" eCBSV Written Consent, for SSA to disclose the SSN verification, Written Consent must meet SSA's requirements that SSA dictates in the eCBSV User Agreement: "Written Consent, including electronic, by which the SSN holder gives SSA permission to disclose SSN Verification results to the Permitted Entity or Financial Institution (or both) in connection with a credit transaction or any circumstance described in section 604 of the Fair Credit Reporting Act (15	Issue resolved.	N/A

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
	U.S.C. § 1681b). The Written Consent must meet SSA's requirements in section IV of [the] user agreement and SSA's regulations." Second, as previously stated, we disagree that the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018 (Pub. L. No. 115-174, referred to as the "Banking Bill") and eCBSV User Agreement identify the *Gramm-Leach-Bliley Act* (GLBA) as the sole, controlling body of rules and regulations. The Banking Bill does not override the privacy expectations and requirements set forth in the Privacy Act and the Social Security Act, as set forth in SSA's regulations, to which SSA is bound.		
Comment #4: Proposed new regulatory and "verification" requirements are a duplicative and unnecessary encroachment into bank regulation by SSA, and conflicts with Federal Information Security Management Act (FISMA) and Federal Risk and Authorization Management Program (FedRAMP) guidance. As well, FIs are already subject to the GLBA, so SSA should not go beyond the GLBA's provisions.	**Response #4:** We have not imposed any new regulatory requirements, and the only verification requirements we are imposing are to ensure the security of data we are providing. SSA notes that both FISMA and FedRAMP allow federal agencies to establish additional security controls in providing for agencies to take a risk-based approach to securing data by providing for information security protections commensurate with the risk.	Clarified that we were not imposing new regulatory or verification requirements.	N/A

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
	The requirement that data is stored within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the U.S. Virgin Islands, and data encryption requirements are well-defined and long-standing safeguards to protect SSA data held by external entities. SSA agrees that the Permitted Entity shall be required to adopt policies and procedures to ensure that the SSN Verification (and associated Consent) are encrypted. The permitted entity should ensure the security and confidentiality of both the SSN Verification and Written Consent in accordance with Federal law (GLBA has a privacy rule FIs must follow). SSA also agrees that the Permitted Entity should have a process in place (quality reviews, internal audits) to ensure they are actually implementing the rules, while recognizing that the government heavily regulate these organizations. SSA notes that the Permitted Entity Certification requires the Permitted Entity to attest they comply with GLBA.		
Comment #5: The BTC stated that the proposed new section III.A.22 of the User Agreement should be re-written as follows, to resolve all of the regulatory overreach issues they	**Response #5:** While SSA disagrees with the characterization of our requirements as "regulatory overreach," we agree to accept the language proposed by the BTC for proposed new	Issue resolved.	N/A

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
described repeatedly and to align the User Agreement with existing GLBA regulatory requirements: "Consistent with its Permitted Entity Certification and existing obligations under the GLBA, the Permitted Entity shall maintain policies and procedures that 1) ensure the security and confidentiality of the SSN Verifications and 2) ensure SSN Verifications that are maintained in a Managed Service Provider or Cloud Service Provider are encrypted at rest and in transit, and 3) assess the sufficiency of these policies and procedures on an ongoing basis. The Permitted Entity must not provide the Managed Service Provider or Cloud Service Provider the key to unencrypt the SSN Verification maintained in their environment."	section III.A.22.		
Comment #6: The BTC asked that the proposed new section V.A.5 of the Technical Specifications and System Security section, as described in Change #3 of the Addendum, should be re-written as follows to align the User Agreement with existing GLBA regulatory requirements: "Consistent with its Permitted Entity Certification and existing obligations under the GLBA, the Permitted Entity	**Response #6:** SSA agrees to accept this new proposed language for section V.A.5.	Issue resolved.	N/A

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
shall maintain policies and procedures to ensure that SSN Verifications are encrypted at rest and in transit. The Permitted Entity shall also ensure that SSN Verifications are stored within the jurisdiction of the United States (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the U.S. Virgin Islands)."			
Comment #7: The BTC asserted 1) The definition of "cloud service provider" is overly broad and conflicts with the User Agreement. The proposed definition of "cloud service provider" is a general definition that is overly broad for purposes of eCBSV. In fact, due to the fact that the definition is extremely broad, it is likely to result in conflicts within the User Agreement and excessive or impossible technical burdens for some Permitted Entities. They also said that 2) SSA's definition of cloud computing is unclear. They requested SSA resolve this by taking the following two actions: 1) Modify the definition of "cloud service provider" to limit it to the specific areas of concern for SSA in the context of eCBSV as follows: "A	**Response #7:** SSA agrees to define "cloud service provider" within the scope of eCBSV. Accordingly, SSA agrees with the BTC's first recommendation, to modify the definition of "cloud service provider" to limit it to the specific areas of concern for SSA in the context of eCBSV as follows: "A third-party company offering cloud-based infrastructure or storage services." (*see page 2)* However, SSA does not agree with the BTC's second point. SSA uses the National Institute of Standards and Technology (NIST) definition of cloud computing (Special Publication 800-145). Therefore, we will not change our current definitions in the User Agreement.	Issue resolved. SSA has made changes where we can do so.	SSA uses the NIST definition of cloud computing, so we cannot change our current definitions in the User Agreement.

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
third-party company offering cloud-based infrastructure or storage services." 2) Add clarifying language to both the definitions of "cloud service provider" and "managed service provider" to indicate that, for purposes of the User Agreement, these definitions do not include "cloud service providers" or "managed service providers" who are Permitted Entities.			

Part II: Comments Relating to Old Material/eCBSV Phase I, Not Proposed eCBSV Phase II

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
Comment #1: An unaffiliated commenter stated that the fee for this service by the government is too low. In addition, the commenter also questioned how the government maintains any kind of privacy for this kind of information. Accordingly, the commenter suggested that banks themselves should perform this service. The commenter also said the government should charge higher fees for the service.	**Response #1:** The type of verification sought here can only be conducted by SSA and is mandated by the Banking Bill. Regarding the eCBSV fees we charge, SSA is required to collect the full cost of eCBSV services. SSA cannot legally profit from eCBSV services. Each Permitted Entity (PE) is required to pay an annual tier-based subscription fee on estimated transaction volume, as well as an administrative fee. We based the fees on forecasted expenses for systems and operational expenses, agency oversight, overhead and the cost to audit each PE by an independent Certified Public Accounting firm. SSA will periodically calculate its costs to provide eCBSV services and adjust the fees accordingly. We will notify PEs in advance of any fee adjustment and post a notice in the Federal Register. This information was described in detail in our 2020 Paperwork Reduction Act submission. Regarding concerns about the privacy of the information we are providing, we note that the eCBSV services are only available to PEs that have a current, valid, and signed User Agreement in place. Each PE is subject to a rigorous authorization and authentication protocol. Each PE must provide SSA with a valid Employer Identification Number (EIN) and qualify as a	SSA addressed the commenter's concerns.	

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
	financial institution under the *Gramm-Leach-Bliley Act* (15 U.S.C. 6809), or service provider, subsidiary, affiliate, agent, subcontractor, or assignee of a financial institution (section 215(b)(4)). Additionally, each PE is required to submit a PE Certification Statement at least every two years. Finally, to verify a Social Security Number (SSN), the PE must have valid written consent that is signed by the SSN holder before the PE submits the SSN holder's name, date of birth and SSN to the eCBSV service. eCBSV will simply return a response of "yes" or "no." If our records show that the SSN holder is deceased, eCBSV will return a death indicator. eCBSV does not verify an individual's identity, nor does it provide further information beyond that described here.		
Comment #2: The BTC requested that SSA should enhance its customer service capabilities for eCBSV users. Specifically, the eCBSV system is intended to be available to Permitted Entities on a near-continuous 24/7 basis, with some periods of scheduled downtime. However, there is currently no adequate customer service support available to address issues which occur during off-times, when SSA is closed. Given that Congress directed Permitted	**Response #2:** eCBSV is and will continue to be available 24/7. If eCBSV users experience technical problems, SSA offers support as soon as possible during that business day, or the next business day. However, the BTC has expressed they would like 24/7 customer service, for both hardware and software support, and that they are willing to pay for it. They expressed this would be helpful for them since the financial industry functions on a 24-hour basis, and users may be located outside of the U.S. time zones.	Tabled for future discussion	Feasibility and resource issues.

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
Entities to pay for the entire cost of the development and upkeep of eCBSV, the BTC believes it is appropriate and necessary for SSA to provide a customer support mechanism at all times. The BTC believes PEs are willing to pay more for more robust service.	SSA understands the BTC's desire for such service. However, this is a major undertaking that is very much outside the scope of SSA's current activities in any area- we do not offer 24/7 service for any of our programs, even those are the core of our mandate as an agency. Since we have no basis on which to calculate 24/7 support costs to impose on the BTC, we would need time to explore feasibility and costs in the areas of hiring, facilities, systems, communications systems, and personnel issues. Accordingly, we believe this is a long-term discussion, and one that will not be resolved during this PRA cycle. However, although we cannot speak to this proposal now, we can agree to explore it further as a long-term goal.		
Comment #3: SSA should accelerate its exploration of how to enhance the matching logic of the eCBSV to provide better information to help fight fraud. Commenting PEs again questioned the type of response eCBSV offers, an issue that was questioned, discussed, and established during the PRA process for eCBSV Phase I. To reiterate, eCBSV does not verify identity. As SSA has made clear, we specify if the name and SSN submitted	**Response #3:** ***Legal Reasons Why We Use the Current Paradigm (Especially Privacy):*** The Privacy Act states that "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains. . . ." 5 U.S.C. § 552a(b). In the case of eCBSV, SSA does not collect and maintain the number holder's consent, which increases risk of improper disclosures for the agency. Consequently, increasing the number of data	SSA will continue to provide the information elements originally described in eCBSV Phase I.	See response for further explanation.

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
to us match each other in our records; if the name/SSN are recorded in our records as being associated with a deceased person, we provide that information. The BTC again asked for more specific information beyond the "yes," "no," or "death" options. They expressed that while a binary "yes" or "no" response is helpful, an eCBSV system that incorporates more sophisticated logic into its core functionality would greatly enhance the effectiveness of the system. For example, SSA could enhance eCBSV by providing a "yes" or "no" response for each of the three pieces Fraud Protection Data submitted by a Permitted Entity in the course of making an SSN Verification request. The BTC expressed that this more descriptive matching response would put users of the eCBSV system in a better position to make more intelligent decision on identity verification of individuals, thereby protecting more consumers from financial and identity fraud. They also asserted the belief that such a change is well within SSA's statutory authority and is in line with	elements upon which the agency verifies and discloses data will increase the agency's risk of improper disclosure. Further, the agency would have to change the consent language in the electronic and paper templates in order to obtain the number holder's informed consent for such granular disclosure. As explained below, the Banking Bill does not require the agency to provide verification of each fraud element and the agency's long-standing practice has been to provide a "Y" or "N" except in very limited circumstances. Thus, we do not see a basis to increase SSA's risk of a wrongful disclosure. In addition, SSA's policies on consent and minimal disclosure are based on the personal and sensitive nature of the public's information. Participation in the social security program is mandatory, so people cannot limit what information is given to us. Therefore, we have traditionally followed a policy of strict confidentiality of our records. Our established framework was developed by balancing the sensitivity of the information; individuals' expectation of confidentiality in the information that they provide to us; and the interest in the disclosure. To ensure appropriate use of Privacy Act-protected data entrusted to us and to remain consistent with our longstanding practice, we will		

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
the stated goal of the Banking Bill.	disclose only a "Y" or "N" per verification request, not for each specific element. ***We Do Not Provide It For Any Other Data Matching:*** In general, we do not provide this data for any other data matching, so it would be problematic to provide it only in this context. ***How Current Paradigm Satisfies Banking Bill Requirements:*** SSA provides millions of SSN verifications a year to public and private entities. Our policy and practice has been to provide a SSN verification as a "Y" or "N." We have limited instances in which SSA discloses more information related to an SSN verification with explicit authorization from the number holder. These exceptions are limited to Federal agencies only. Further, our current SSN verification practice satisfies our obligations under section 215 of the Banking Bill. The Banking Bill does not require us to alter SSA's longstanding framework for SSN verifications to public and private entities based on the number holder's written consent. Section 215 of the Banking Bill does not speak to whether SSA must provide a "yes" or "no" response for each Fraud Protection Data element a permitted entity submits and does not require SSA to modify the database or process to provide a reason for a "no match." SSA's eCBSV service, by providing the match/no match		

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
	response, "compare[s] fraud protection data … against such information maintained by [SSA] in order to confirm (or not confirm) the validity of the information provided." See section 215(d)(1)." The eCBSV service as it is currently designed (to give a yes/no response), is "reasonably designed to effectuate the purpose of [section 215 of the Banking Bill]." Accordingly, we will maintain our established SSN framework. ***Explanation of How BTC's Proposal Does Not Really Combat Synthetic Identity Fraud:*** Our current data provided to PEs ensures they make objective-based decisions regarding the results of verification requests submitted. By providing more granular "Y/N" for each data element submitted, we introduce subjectivity into the PE decision-making process (i.e., PEs can potentially treat certain combinations of matches/no matches differently). Some combinations of matches/no matches may be the result of typos, colloquial/nicknames, etc. However, other data-specific no matches may be the result of fraud and, therefore, could negatively impact the number holder as well as contradict the intent of the Banking Bill.		

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
Comment #4: **SSA should create consistency in consent language requirements for all user experiences – digital and paper.** Last year, OMB and SSA finalized a User Agreement for eCBSV containing approved Written Consent templates, which are memorialized in Exhibit C of the User Agreement. Given the effort that led to this successful outcome, the BTC believes it would be appropriate to allow this approved language to be incorporated into paper-based consumer credit applications, obviating the need for a separate Form SSA-89. This would greatly enhance the user experience for consumers, likely reducing confusion, and reduce burdens for Permitted Entities by streamlining the process for obtaining consumer consent prior to accessing eCBSV.	**Response #4:** SSA agrees to amend the eCBSV User Agreement to allow PEs/FIs to use the Written Consent Template language in the PE's/FI's paper business process. However, we caution that it is our legal opinion that on its own, the Written Consent Template does not constitute sufficient consent as it does not contain the other consent requirements in Section IV of the eCBSV User Agreement, i.e., does not include the Fraud Protection Data on that form and does not include the signature of the consenting individual. To be sufficient consent, the Written Consent Template language must include all the requirements listed in Section IV of the User Agreement and SSA's regulations (i.e., the consent must be associated with the number holder's name, date of birth, and SSN; Exhibit C, Written Consent Template language, , the specific purpose for the SSN Verification, and a valid signature). We also note that the BTC did not appear to have offered substantiated reasons for their request to incorporate the Exhibit C Written Consent Template language of the eCBSV User Agreement into their paper-based business process. Regardless, SSA will allow this request, but will continue to offer and encourage the use of the SSA-89 as the most valid form of written consent.	SSA agrees to amend the eCBSV User Agreement to allow the use the Written Consent Template language for the paper (CBSV) process. However, we strongly encourage PEs and FIs to continue to use the SSA-89.	N/A

Part III: Minor Technical Issues/Misunderstandings for eCBSV Phase II, All of Which Are Resolved/Clarified

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
Comment #1: The BTC noted that we changed the Permitted Entity Certification to eliminate the specific reference for detailed Permitted Entity definition, and only reference the generic Banking Bill. This appears to leave Service Providers (SP) in the position of providing sufficient reference for clients to determine eligibility (a search using the term Banking Bill performed on 1/12/2021 returned a reference to a 2020 piece of legislation, rather than the one related to eCBSV). The BTC asked if, based on that information, the change was intentional? If so, does it affect who can participate in the eCBSV Program?	**Response #1:** SSA did not make any changes to the Permitted Entity Certification (PEC). The correct PEC template is in Exhibit A in the User Agreement. We are using the same template in the Customer Connection. There was an extra PEC template for the initial rollout only on the eCBSV website; however, we will remove that older version to alleviate any confusion.	Issue Resolved.	N/A
Comment #2: The BTC noted that in the Permitted Entity Certification, the "Financial Institution Registration" section, SSA does not specifically state that only Financial Institutions (FI) are eligible to participate. While SSA provides a hyperlink to learn more about Permitted Entity Certification, the documentation provided lacks ability to explore that link. The commenters then asked: does this link provide sufficient detail related to Permitted Entity qualification? In addition, for clarity and simplicity, the commenters suggested that SSA add the requirement that participation through an SP is limited to FIs.	**Response #2:** The link on the screen will direct the user back to the eCBSV Website where there is information about the onboarding process, including the FI Registration process. SSA appreciates the suggestion and we will consider it for a future update.	SSA ensured the link on the screen directs the user back to the onboarding process on the eCBSV website. SSA will consider the suggestion of adding the requirement that participation through an SP is limited to FIs for a future update.	N/A

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
Comment #3: The BTC observed that the FI Registration completion notice provides advice to download and save the completed PE certification, but not the Employer Identification Number (EIN) Consent form, nor does it advise the respondents to share copies with the SP. The BTC's assumption is the SP needs the EIN to supply to SSA prior to initiation of traffic to eCBSV. Therefore, giving the advice to share with SP would be helpful here. The BTC requested that SSA provide the full package of documents required by the PE, and advise that if the PE is coming through an SP, that they share those documents SSA will require of the SP.	**Response #3:** The requirement for SPs to manually provide SSA with the EINs of the FI they serve, prior to submitting traffic, was for the Initial rollout only. In the Expanded rollout, FIs will use the FI Registration screen to register their entity with SSA. Once this is complete, that FI will be registered to use eCBSV through an SP. SPs will need to send the EIN associated to the transaction when making a request. It will be on each SP to obtain the FI's EIN as part of their internal business process when adding on FIs.	SSA explained the new process under eCBSV Phase II will differ from Phase I, as we included a specific FI Registration page for this purpose. The SPs will need to obtain the FI's EIN as part of their internal business process.	N/A
Comment #4: The BTC remarked that the online enrollment process for FIs using SP does not require entry of the name of the intended SP. They stated that, because SSA is not requiring that information, it is unclear how the SP will ensure that Item #1 from the current User Agreement is complete. Similarly, there is no obvious mechanism for providing the notice of intended use of SPs by an FI (#11 from User Agreement) via the Portal screens. They are asking SSA to please clarify this.	**Response #4:** Per our response above to Comment #3, the FI does not need to indicate the SP they plan to use. Once they are registered, they can use whichever SP they choose. The SP is required to provide the EIN of the FI where the transaction is coming from. If that FI has not previously registered, the verification service will not process the transaction.	SSA reiterated that FIs will not need to indicate the SP they plan to use on their registration page, and that the SP the FI chooses will be required to provide the EIN of the FI. In addition, eCBSV will only process transactions for registered FIs.	N/A

Commenter Concern	SSA Response	Final Resolution of Issue	Reason for Inability to Fully Compromise, If Applicable
Comment #5: The BTC pointed out that SSA's sample Entity Registration email contains a reference to a real entity. They requested that SSA's samples avoid references to any real corporate entities. **(*Note: This was on SSA's website, not in any other eCBSV materials.)***	**Response #5:** SSA appreciates this observation, and we will update the sample to remove the reference. We will avoid making any references to real corporate entities in the future.	Issue Resolved.	N/A