Generic Clearance for the Collection of Social Media Identifier(s) on Immigration Forms - Responses to 30-day Public Comments

Public Comments (regulations.gov): USCIS-2025-0003
30-day FRN Citation (federalregister.gov): 90 FR 44693
Publish Dates: September 16, 2025 – October 16, 2025

Comment ID	Comment Sub-Theme	Comment Summary	USCIS Response
Topic 1. Legal Authority to Collect			
1264 1273	Violating EO's	The comments argue that the proposed Social Media Collection rule violates executive orders, constitutional rights, federal laws, and international human rights obligations. Key points include: **1. Violation of Executive Authority:** The rule exceeds the scope of the President's powers, as executive orders must derive authority from the Constitution or an act of Congress. EO 14161, Protecting the United States From Foreign Terrorists and Other National Security and Public Safety Threats, is cited as insufficient to justify the rule, and the rule allegedly encroaches on Congress's lawmaking authority. **2. Conflict with EO 13107:** The comments argue that the proposed rule violates U.S. obligations under the International Covenant on Civil and Political Rights (ICCPR) and EO 13107, Implementation of Human Rights Treaties, by failing to respect human rights, imposing conditions on fundamental rights (e.g., freedom of speech, assembly, and privacy) without meeting strict scrutiny standards, and lacking necessity and proportionality as required by both U.S. law and international treaties. Overall, the comments urge abandonment of the rule due to its legal, constitutional, and procedural deficiencies.	**Response:** For responses regarding constitutional issues and human rights, please see ***Topic 6., Constitutional Issues***, below. Federal laws, including the Immigration and Nationality Act (INA) and Homeland Security Act of 2002, provide authority for this information collection. For example, INA § 287(b), 8 U.S.C. § 1357(b), and 8 C.F.R. § 287.5(a)(2) empower officers and agents to "take and consider evidence concerning the privilege of any person to enter, reenter, pass through, or reside in the United States." Similarly, for naturalization purposes, INA § 335, 8 U.S.C. § 1446, empowers any employee of USCIS to conduct a personal investigation of the person applying for naturalization, take testimony concerning the admissibility of the applicant for naturalization, and require the production of relevant books, papers, and documents. Details about collected data, including how USCIS uses information, shares information and protects information are provided publicly via Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs) on the DHS website. Each USCIS form also has a DHS Privacy Notice that details the authority of DHS to collect information, its purpose, when it may be disclosed, and applicable routine uses. To ensure compliance with these policies, USCIS officers must complete annual training on the operational use of social media and sign a Rules of Behavior document. Additionally, DHS will not request user passwords in furtherance of this collection and will not violate or attempt to subvert individual privacy settings or controls individuals may have implemented on social media platforms. Consistent with the requirements of the Privacy Act (5 U.S.C. § 552a(e)(7)), DHS does not maintain records "describing how any [citizen of the United States or alien lawfully admitted for permanent residence] exercises rights guaranteed by the First Amendment, unless expressly authorized by statute or by the individual about whom the record is maintained

			or unless pertinent to and within the scope of an authorized law enforcement activity." Furthermore, DHS policy directs that "DHS personnel shall not collect, maintain in DHS systems, or use information protected by the First Amendment unless (a) an individual has expressly granted their consent for DHS to collect, maintain and use that information; (b) maintaining the record is expressly authorized by a federal statute; or (c) that information is relevant to a criminal, civil or administrative activity relating to a law DHS enforces or administers. In addition, DHS personnel should not pursue by questioning, research, or other means, information relating to how an individual exercises his or her First Amendment rights unless one or more of the same conditions applies." DHS components must also adhere to DHS Directive 110-01, "Privacy Policy for Operational Use of Social Media," and DHS Instruction 110-01-001, "Privacy Policy for Operational Use of Social Media," which define the authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness; investigating an individual in a criminal, civil, or administrative context; assessing a person's eligibility for a benefit; making a personnel determination about a Department employee; making a suitability determination about a prospective Department employee; or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. This policy also requires DHS Operational Components to receive approval from the DHS Privacy Office regarding the privacy implications of any planned operational use of social media to ensure that it is compliant with Departmental privacy policies and standards.[1] DHS employees, who are permitted and trained to utilize social media for operational purposes during the performance of their duties, must adhere to DHS privacy policies, as established by the Chief Privacy Officer. DHS maintains a framework of safeguards, training, and policies for use of social media in vetting programs and to ensure preservation of privacy, civil rights, and civil liberties. When adjudicating eligibility to travel to or be admitted to the United States and for immigration

[1] DHS authorities for the "Privacy Policy for Operational Use of Social Media" are as follows: Public Law 107-347, "E-Government Act of 2002" as amended, Section 208, codified at 44 U.S.C. § 3501 note; 5 U.S.C. § 552a, Records Maintained on Individuals, (The Privacy Act of 1974, as amended); 6 U.S.C. § 142, Privacy Officer; 44 U.S.C., Chapter 35, Subchapter III, "Information Security" (The Federal Information Security Management Act of 2002, as amended); Delegation 13001, "Delegation to the Chief Privacy Officer."

			benefits, the use of social media is governed by strict privacy provisions, use limitations, and in adherence with all constitutionally protected rights and freedoms.[2] DHS Oversight Offices, including the Office of the General Counsel, the Privacy Office, and the Office for Civil Rights and Civil Liberties, each review aspects of DHS policies regarding the use of social media information. They regularly advise programs on best practices and methods for ensuring legal and policy compliance. In addition, the USCIS Privacy Office reviews and must approve each office's operational use of social media and associated activities. Employees in these offices are required to take designated training, sign a Rules of Behavior document, and obtain a Privacy Impact Assessment governing the program's specific operational use of social media before implementation.
Topic 2. Compliance with the PRA			
1263 1264 1268 1271 1275 1277	Practical Utility	The comments collectively argue that the proposed collection of social media identifiers lacks practical utility for several reasons: **1. Failure to Demonstrate Necessity**: DHS has not provided evidence that collecting social media identifiers is essential to its core functions or that it enhances national security or public safety. Existing vetting processes, such as criminal background checks, are already sufficient for assessing applicants' eligibility and risks. **2. Unreliable and Ineffective Data:** Past pilot programs by DHS have shown that social media screening has not provided actionable or reliable information for vetting purposes. Social media content is often difficult to verify for authenticity, context, or relevance, making it an unreliable tool for evaluating applicants. **3. Excessive Burden:** Collection imposes significant burdens on applicants, requiring them to recall years of social media accounts. It also creates inefficiencies for adjudicators, who must manually review vast amounts of irrelevant or unverifiable data, detracting from their ability to focus on more effective vetting processes. **3. Irrelevant Time Frame:** Proposed five-year period for social media disclosure is excessive and often unrelated to the specific immigration benefit being sought. For example, requiring five years of data for a two-year conditional green	**Response:** 5 CFR 1320.9 states, "As part of an agency's submission to OMB of a proposed collection of information, the agency," in this case, USCIS, "… shall certify… that the proposed collection of information" "(a) [i]s necessary for the proper performance of the function of the agency, including that the information to be collected will have practical utility." This collection will have immediate practical utility to determine an individual's eligibility for the immigration benefit(s) they seek. Social media is a prominent component of modern society and DHS's efforts to protect the homeland must evolve as society evolves. Given the nature of DHS's mission, it is important for DHS to ask for and review this information. All information provided by an individual may be used to vet the parties to a benefit request, including applicants, derivatives, and beneficiaries. In addition to checking against government information, DHS officers may use publicly available information, including social media information, as part of the existing vetting process to verify the information submitted. If an initial screening indicates possible information of concern or a need to further validate information, a trained officer will have timely visibility of the publicly available information on the platforms associated with the social media identifier(s) provided by the applicant, along with other information and tools these officers regularly use in the performance of their duties. The officer will review provided

[2] All access controls described in relevant Privacy Impact Assessments and System of Records Notices are available to the public on the DHS website (www.dhs.gov/privacy).

		card is untethered to the purpose of the application. **Recommendations for Improvement:** • Tailor the collection to specific forms and types of immigration relief to ensure relevance. • Adopt a targeted, risk-based approach to social media screening, reserving it for cases with specific risk indicators rather than blanket collection. • Establish clear guidelines for adjudicators to evaluate social media data objectively and consistently.	identifiers on the relevant platforms in a manner consistent with the privacy settings the individual has chosen to adopt for those platforms. Social media may be used to support or corroborate application information, which will help USCIS' mission to administer the nation's lawful immigration system by providing an additional means to adjudicate issues related to relevant questions about identity, occupation, previous travel, and other factors. It may also be used to identify potential deception or fraud. Further, it may help detect potential threats because criminals and terrorists, whether intentionally or not, have provided previously unavailable information via social media that identified their true intentions. Social media may therefore help distinguish individuals of additional concern from those individuals whose information substantiates their eligibility for travel to or entry into the United States or immigration benefits. In addition, generally other than discretionary overseas denials, USCIS would not deny a benefit based on social media information without first confronting the applicant, petitioner, or benefit requestor with the information and providing an opportunity to explain it or rebut any negative inferences USCIS may have drawn from it. See 8 C.F.R. § 103.2(b)(16)(i) and (ii). DHS disagrees that it should define specific criteria under which individuals may be subject to social media vetting and believes that social media screening is best applied to requests for an immigration benefit requiring a background investigation. Social media involves publicly available information that is accessible to anyone without a warrant and DHS would not be unique in reviewing it. Along with checking against government systems and information, DHS officers may use publicly available information, social media included, as part of the vetting and screening process to verify the information submitted. Moreover, the content of an individual's public social media can be used to assess and identify immigration fraud, bars to eligibility, and national security and public safety threats, requiring vetting procedures that are as broad as possible. Limiting searches of social media, such as implementing reasonable suspicion requirements, would hinder DHS in its vetting efforts for these legitimate purposes.
1263 1264 1265 1268 1270	Underestimation of Burden	The comments collectively highlight significant concerns regarding the burden imposed by the proposed collection of social media identifiers. Key points include:	**Response:** In USCIS' response to the public comments from the 60-day notice, as published in the Federal Register at 90 FR 11324 on March 5, 2025, the estimated hour burden per response was increased by an additional 0.59 hours for

1271 1273 1275 1276 1277		**1. Underestimated Time Burden:** USCIS significantly underestimates the time burden for applicants to recall and provide social media identifiers from the past five years. Many individuals cannot realistically reconstruct all accounts, usernames, or platforms, especially if they were abandoned, forgotten, or created under pseudonyms. The process may involve contacting service providers, reviewing past records, or reaching out to family members, which is further complicated by language barriers, unreliable internet access, and lost login information. **2. Vagueness and Lack of Clarity:** The definition of "social media identifiers" is vague, and no clear list of platforms is provided, leaving applicants uncertain about what to disclose and creating inconsistent reporting by applicants. **3. Impact on Vulnerable Populations:** Victims of abuse, trafficking, and asylum seekers face unique challenges, such as having multiple accounts created under coercion, loss of access to accounts, fear of endangering loved ones, or estrangement from their families, making compliance challenging and risking unfair denials. **4. Unrealistic Cost Estimates:** Claim that the collection imposes no financial cost is criticized as implausible. The additional hours required for applicants to comply with the proposal will result in significant hidden costs in terms of time and resources. **Recommendations:** • Reassess time and cost estimates for applicants or significantly revise to minimize the burden. • Define "social media identifiers" and limit the scope to current, verifiable accounts. • Ensure collection process accounts for difficulties vulnerable populations face in providing this information. • Implement grace period for applicants to understand and comply with new requirements.	each impacted information collection to more accurately reflect the burden imposed on the public, with the exception of the Form I-131 where an additional 1.09 hours were added and the Form I-751 where an additional 3.09 hours were added. Based on the proposed collection of social media identifier(s), the estimated hour burden per response to complete these forms will have an overall increase by an average of 1 hour on each form. USCIS closely reviewed the estimated average hour burden per response based on where social media identifier(s) are being added and instructional content added to allow the respondent to provide the requested information, as necessary, and is confident that this increase in burden addressed the commenters' concerns to more accurately reflect the burden estimate. It is projected that the proposed collection of social media identifier(s) will have a minimal impact for many respondents because most social media users do not utilize multiple accounts within a given platform or change usernames regularly. Individuals are not expected to include accounts designed for use by multiple users within a business or other organization. If an individual has multiple accounts on multiple platforms, they must provide that information to the best of their ability. As addressed in USCIS' response to the public comments from the 60-day notice, as published in the Federal Register at 90 FR 11324 on March 5, 2025, to provide clearer guidelines on the proposed collection of information, USCIS updated the form instructions for each affected information collection to provide more detailed instructional content on the social media identifier(s) question(s), including how the Department defines social media and examples of social media platforms. The estimated total annual cost burden associated with a specific information collection will be captured in those approved collections. Any updates to the estimated annual cost burden to respondents, which includes the imposed out-of-pocket costs to respondents, will be outlined in each Supporting Statement for the affected information collection. Out-of-pocket costs may include payments for document translation and preparation services, attorney and legal fees, postage, and costs associated with gathering documentation. In addition, any updates to the estimated cost to the federal government will be outlined in each Supporting

			Statement for the affected information collection.
1271	Duplication	The comments argue that the proposed collection of social media identifiers is duplicative for the following reasons: **1. Redundancy:** • DHS already has access to extensive applicant data through existing systems, including biometric data, travel records, law enforcement databases, and even social media data collected during prior applications. • Applicants often provide the same information multiple times throughout the immigration process. Requiring the same information again for subsequent applications (e.g., for permanent residency or citizenship) is unnecessary. **2. Unnecessary Burden**: Duplication of information collection imposes an additional and unnecessary burden on applicants, who must recall and provide the same data multiple times. **Conclusion:** The proposed collection is duplicative of data DHS already possesses, offers little additional value for screening purposes, and imposes an unnecessary burden on applicants by requiring redundant and often irrelevant information.	**Response:** The proposed information collection is not duplicative because social media identifier information has not been consistently collected in the past. Further, social media data may provide information that is not available through existing systems. Information found on social media via the provision of social media identifier(s) will enhance the vetting process and identify potential threats. For example, social media may be used to support or corroborate a benefit seeker's application by providing an additional means to adjudicate issues related to relevant questions about identity, occupation, previous travel, and other factors. It may also be used to identify potential deception or fraud. Further, it may help detect potential threats because criminals and terrorists, whether intentionally or not, have provided previously unavailable information via social media that identified their true intentions. Social media may therefore help distinguish individuals of additional concern from those individuals whose information substantiates their eligibility for travel to or entry into the United States or immigration benefits. Additionally, DHS has taken into account the burden involved in collecting this information and has found this burden is reasonable and justified given the security and fraud prevention benefits from this collection. Please see further responses addressing burden in ***Topic 2. Compliance with the PRA****, Underestimation of Burden.*
1271	Appropriateness of generic clearance	The comments argue that the use of generic clearance for the proposed collection of social media identifiers is inappropriate for the following reasons: **1. Not Voluntary:** Generic clearance is intended for voluntary collections, but the proposed collection is mandatory for applicants seeking immigration benefits. Failure to comply could result in adverse consequences, making it unsuitable for generic clearance. **2. Not Low Burden:** Collection imposes a significant burden on applicants, requiring them to recall years of social media activity, navigate unclear requirements, and potentially obtain information from third parties. DHS's estimate of 40 minutes per applicant is criticized as unrealistically low, and the burden cannot reasonably be characterized as "low."	**Response:** The process used by DHS to obtain this generic clearance is similar to, but no less demanding than, the process to obtain approval of any new or revised information collection as it still requires the standard 60 and 30-day notice process. In addition, a generic information collection clearance requires the same level of justification, support, analysis, and level of approval as any other information collection approved by the Office of Management and Budget under the Paperwork Reduction Act and implementing regulations.[3] This generic clearance is being used to propose the collection of social media identifier(s) on the affected information collections. This method provides a single docket for the public to provide comments on the proposed collection of social media identifier(s) and affected information collections, which reduces the burden on the public, rather than the public having to identify and comment

[3] 44 U.S.C. chapter 35; 5 CFR Part 1320.

		3. Highly Controversial: The proposed collection is highly controversial and represents a significant policy change. Unlike the uncontroversial collections typically approved under generic clearance (e.g., customer service surveys), this proposal raises concerns about constitutional rights, including free speech, privacy, and due process. Similar proposals, such as the State Department's collection of social media identifiers, have faced widespread public opposition. Additionally, the proposal affects millions of people annually, including U.S. citizens and their relatives, making it far more substantive and impactful than the low-stakes collections typically eligible for generic clearance. Overall, the comments assert that the proposed collection does not meet the criteria for generic clearance due to its mandatory nature, high burden, controversial implications, and significant policy impact. Pursuing expedited approval under generic clearance is deemed wholly inappropriate and fails to account for the scope and significance of the proposal.	on a separate notice and docket for nine separate information collections. The use of a generic clearance also reduces burden and cost to the Federal government to publish separate Federal register notices. USCIS agrees that a generic clearance is usually used for information collections that are voluntary, low-burden, and non-controversial.[4] As per requirements under 44 U.S.C. 3501 *et. seq*. and 5 CFR 1320, USCIS believes that a generic clearance is appropriate to use for this process in order to make the proposed necessary changes to enable and help inform national security and public safety screening, and vetting, and related inspections. USCIS published a 60-day Federal Register Notice and 30-day Federal Register Notice for the New Collection of Social Media Identifier(s) on Immigration Forms. The 60-day notice and the 30-day notice included each affected information collection instrument with instructions which included the proposed changes on the Federal eRulemaking Portal site at: *https://www.regulations.gov* and entering USCIS-2025-0003.
Topic 3. Compliance with the Privacy Act/Records Act/Information Security/Data Integrity			
1264 1265 1271 1272 1273 1275 1276	Privacy Violation	The comments collectively raise significant concerns about privacy violations. Below is a summary of the key issues: **1. Violation of Individual Privacy:** Commenters assert that social media identifiers are categorized as Sensitive Personally Identifiable Information (SPII), and their collection could lead to harm, embarrassment, or unfairness to individuals. **2. Inconsistency with the Privacy Act of 1974** • **Relevance and Necessity**: Collection of social media identifiers fails to meet the Privacy Act's requirement that federal agencies collect only information proven to be relevant and necessary for lawful purposes like immigration adjudication or national security. • **Transparency**: Proposed collection lacks clear guidance on how the information will be used, stored, or shared, which violates the Privacy Act's requirement to inform individuals about the routine uses of their information and the consequences of non-disclosure. **3. Data Security Risks:** The lack of robust safeguards increases the risk of data breaches,	**Response:** DHS disagrees with commenters who believe collection of social media identifiers is a violation of privacy and leads to potential misuse of information for vulnerable and other populations. Any information provided by an individual on a form is done so voluntarily by the individual. In this case, Information requested by DHS is used for purposes of adjudicating the requested immigration benefit. DHS does not compel individuals to request immigration benefits from USCIS. Details about collected data, including how USCIS uses information, shares information and protects information are provided publicly via Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs) on the DHS website. Each USCIS form also has a DHS Privacy Notice that details the authority of DHS to collect information, its purpose, when it may be disclosed, and applicable routine uses. As previously explained, DHS components must also adhere to additional guidelines and requirements when engaging in the operational use of social media. This policy requires DHS Operational Components to receive approval from the DHS Privacy Office regarding the privacy implications of any planned operational

[4] 8 CFR 1320.3(c)(1); Sunstein, Cass R., *Memorandum for the Heads of Executive Departments and Agencies, and Independent Regulatory Agencies: Paperwork Reduction Act – Generic Clearances* (May 28, 2010).

		misuse, and retaliation, while DHS's oversight mechanisms are deemed inadequate to protect sensitive information. **4. Legal and Ethical Concerns:** • **Unlawful Surveillance:** Comments argue that the proposed collection amounts to state-sponsored mass surveillance, which infringes on constitutional rights and privacy expectations. • **Lack of Privacy Assessment:** DHS has not conducted a sufficient Privacy Impact Assessment (PIA) as required by the E-Government Act of 2002, nor has it provided adequate notice through a System of Records Notice (SORN). **Recommendations:** **1. Ensure Compliance with the Privacy Act**: Limit data collection to information that is demonstrably relevant and necessary for lawful purposes. **2. Conduct Privacy Assessments:** Perform thorough Privacy Impact Assessments (PIAs) and update System of Records Notices (SORNs) to identify risks and ensure compliance with privacy laws. **3. Implement Robust Privacy Protections**: Establish comprehensive protections for the collection, storage, use, and sharing of social media information to prevent data breaches, unauthorized access, and misuse of personal information. **4. Limit Scope and Duration of Data Retention:** Limit the retention period for social media data to prevent indefinite monitoring of individuals and ensure sharing is restricted to entities directly involved in immigration adjudication and national security. **5. Increase Transparency**: Inform individuals about the routine uses of their social media data and the consequences of non-disclosure. **6. Improve Oversight and Accountability**: Reestablish internal oversight mechanisms, such as DHS's Office for Civil Rights and Civil Liberties, to safeguard privacy and civil liberties.	use of social media to ensure that it is compliant with Departmental privacy policies and standards. DHS employees, who are permitted and trained to utilize social media for operational purposes during the performance of their duties, must adhere to DHS privacy policies, as established by the Chief Privacy Officer. DHS Oversight Offices, including the Office of the General Counsel, the Privacy Office, and the Office for Civil Rights and Civil Liberties, each review aspects of DHS policies regarding the use of social media information. They regularly advise programs on best practices and methods for ensuring legal and policy compliance. In addition, the USCIS Privacy Office reviews and must approve each office's operational use of social media and associated activities. Employees in these offices are required to take designated training, complete a Rules of Behavior document, and obtain a Privacy Impact Assessment governing the program's specific operational use of social media before implementation. DHS will only be viewing publicly available information on the platforms associated with the social media identifier(s). DHS will not be making requests of the social media platforms to violate an individual's privacy settings to help establish the individual's eligibility for travel, entry, or benefits. Additionally, DHS will not collect social media passwords from individuals. DHS will make case-by-case determinations based on the totality of the evidence. DHS has a layered approach to security and any social media identifiers collected would be only one piece of a large mixture of information used in the analysis of eligibility for the requested immigration benefit. Though there may be the potential for an individual to provide false or inaccurate information, the answers (or lack thereof) provided in conjunction with the other information considered will help inform our direction of inquiry.
1265 1271	Connections Not Giving Consent	The comments provided raise several concerns about the collection of social media identifiers, particularly in the context of evaluating immigration-related benefits. Below is a summary of the key points made in the comments regarding connections not giving	**Response:** DHS regularly collects information about aliens, U.S. citizens, and children in the course of adjudicating an immigration request. This also includes information about third parties that may be associated with a subject individual. As discussed before, DHS provides appropriate notification to individuals, including those

		consent for the collection of social media information: **1. Lack of Consent:** Collecting social media identifiers not only impacts the individual applicant but also infringes on the privacy of their connections (e.g., friends, family members, or others whose information or photos may appear on the applicant's social media). These individuals likely have not consented to their information being accessed or reviewed by government officials. Connections whose information is indirectly collected may have no control over how their data is stored, shared, or used. **Recommendations:** **1. Avoid Collecting Social Media Identifiers**: Do not collect social media identifiers for immigration-related benefits, emphasizing that this practice infringes on the privacy of both applicants and their connections who have not consented to their information being accessed. **2. Respect Privacy Rights**: DHS should consider the privacy rights of individuals and their connections, ensuring that sensitive information is not collected or retained without explicit consent.	covered by the Privacy Act, by publicly issuing PIAs, SORNs, and publishing privacy notices on individual forms. Further, the information that DHS may access via social media is publicly accessible and DHS may not access information that is designated as private. DHS does not specifically target children's information but may collect it if relevant to a case. DHS does not exclude any category of individual from its review of publicly available information on social media sites. Social media platforms provide opportunities to gain valuable insights into individuals' movements, relationships, and behaviors. DHS can use the content of individuals' public social media to assess and identify immigration fraud or other bars to eligibility for particular immigration benefits, as well as potential national security and public safety threats. DHS acknowledges that some of the individuals impacted will be United States citizens, however collecting social media information from U.S. citizen petitioners is within the scope of the authority of DHS. In many circumstances, the alien's relationship to a United States citizen is material to the benefit sought. The Immigration and Nationality Act (INA) authorizes DHS to collect information needed to assess eligibility for an immigration benefit. USCIS notes that the information collected will assist USCIS to evaluate information key to benefit eligibility. In many circumstances, this will involve information from a United States citizen who has filed an immigration benefit request on behalf of an alien.
1265 1271 1275	Data Integrity	The comments specifically address data integrity concerns in the following ways: **1. Accuracy and Misinterpretation Risks**: Social media data is often unreliable and does not accurately represent an individual's identity or behavior. Posts can be misinterpreted as threats or negative behavior due to lack of context, cultural nuances, or officials' limited understanding of social media trends and language. This undermines the reliability and accuracy of using social media information for vetting purposes. **2. Risk of Bias**: Access to expansive social media data raises concerns about bias in decision-making and the potential for abuse, particularly if data is used beyond its intended purpose or without proper checks.	**Response:** DHS takes precautions to maintain the security, confidentiality, and integrity of all information collected about individuals. Safeguards include controls that limit information access to only authorized users. These safeguards employ advanced security technologies to protect the information stored on our systems from unauthorized access. To ensure compliance with these policies, USCIS personnel complete training on the operational use of social media and sign the Operational Use of Social Media Rules of Behavior before any social media use and annually thereafter, if operational use of social media is a continuing requirement. The data collected by USCIS will be safeguarded and stored in accordance with DHS/USCIS-007 Benefits Information System, see 84 FR 54622 (October 10, 2019) and DHS/USCIS-010 Asylum Information and Pre-Screening

		3. Subjective Discretion: Reviewing officers may have unfettered discretion to interpret social media activity, increasing the risk of bias and inconsistent decisions. **Recommendations:** **1. Avoid Collecting Social Media Identifiers:** Withdraw the proposal to collect social media identifiers entirely, as the data is unreliable, prone to misinterpretation, and not suitable for immigration-related determinations. **2. Establish Clear Guidelines**: DHS should provide explicit criteria for how social media data will be collected, analyzed, and used to prevent misinterpretation, bias, or misuse. This includes defining what constitutes relevant information and ensuring proper training for officials on social media trends, language, and cultural nuances to minimize misinterpretation of data, risk of bias, and inconsistent decisions.	System of Records, see 80 FR 74781 (November 30, 2015). DHS is aware that social media information can be hacked, manipulated, or falsified. As stated before, DHS will use information from social media as one of several types of evidence that may be used to support or corroborate information about an individual. It may also be used to identify potential deception or fraud. In addition, generally other than discretionary overseas denials, USCIS would not deny a benefit based on social media information without first confronting the applicant, petitioner, or benefit requestor with the information and providing an opportunity to explain it or rebut any negative inferences USCIS may have drawn from it. See 8 C.F.R. § 103.2(b)(16)(i) and (ii).
Topic 4. Administrative Procedure Act (APA)			
1264 1270		The comments argue that the proposed Social Media Collection violates the Administrative Procedure Act (APA) by being arbitrary, capricious, and inadequately justified. Key concerns include the lack of supporting data, failure to consider burdens on applicants and vulnerable populations, unrealistic cost estimates, and the blanket application of requirements across all immigration forms. The rule lacks a clear connection between the data collection and its stated goals, and fails to provide a rational explanation or address public concerns raised during the notice-and-comment period. Recommendations include tailoring the collection to specific forms, defining terms clearly, limiting data collection to relevant cases, and implementing a grace period. Without addressing these issues, commenters assert that the rule would likely fail judicial review under the APA.	**Response:** USCIS disagrees that this collection of information violates the Administrative Procedure Act. USCIS' statutory and regulatory authorities permit the agency to request information necessary for determining eligibility for an immigration benefit. Here, USCIS is asking for additional data points to enhance vetting that it already lawfully conducts. For responses regarding burden and practical utility, please see responses in ***Topic 2. Compliance with the PRA****, Practical Utility* and *Underestimation of Burden.*
Topic 5. Impacts on Immigration Benefit Processing/Travel			
1265 1268 1271	Delay Benefit Processing	The comments suggest that collecting social media identifiers could delay benefit processing due to the following reasons: **1. Increased Workload**: Adjudicators face an increased workload to review and verify vast amounts of potentially irrelevant or unverifiable data, which could detract from their ability to focus on more targeted and effective vetting processes. Random and varied usage of social media platforms (e.g., for personal connections, business, or entertainment) makes them unreliable tools for assessing security threats. This could lead to unnecessary investigations and	**Response:** Any checks of an individual's publicly available social media information will occur concurrently with and not after the current processing steps for a particular benefit request. While it may require some more time up front, DHS believes adding social media questions may reduce processing times overall in many situations as it will allow USCIS to timely use publicly available social media information to support vetting and adjudication programs and identify eligibility, national security, and public safety issues early in the immigration process, rather than later on when resolution of any potential issues may require a greater

		additional work for officials, further slowing down the adjudication process. **2. Misinterpretation and Complexity**: Social media content is often misleading and may not accurately represent an individual. Officials may lack the training or expertise to interpret the constantly changing trends, language, and expressions on social media, further complicating the review process and causing delays. **Recommendations:** **1. Focus on Reliable and Relevant Information**: DHS should prioritize collecting and reviewing information that is demonstrably relevant, necessary, and efficient for determining eligibility for immigration benefits, rather than relying on complex and misleading social media data. **2. Streamline Processes**: Avoid implementing procedures, like social media reviews, that add unnecessary complexity and increase the workload for officials, thereby slowing down benefit processing. Ensure adjudicators have clear criteria for evaluating social media data, minimizing the risk of misinterpretation or bias.	investment of DHS time and resources. This will further supplement other information and tools that trained USCIS personnel regularly use in the performance of their duties to identify issues quickly, early, and efficiently. DHS defines social media as the "sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact." Social media vetting, which has added an overall negligible amount of time to USCIS processing, has been in effect on a smaller scale since 2017 and performed only by trained officers. Officers who are responsible for conducting social media vetting sign agreements outlining Rules of Behavior and receive several annual trainings on privacy requirements and principles, and training specifically related to social media vetting, including how to identify First Amendment activity. These trainings must be completed prior to accessing social media and trained officers must use government-issued equipment to access social media for government purposes. For additional information on how USCIS uses social media, please see the Privacy impact Assessment found at https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-013-01-fdns-august2019.pdf. USCIS will continue to provide resources and training to employees to ensure comprehensive, prudent, and efficient social media screening in the future and monitor resource allocation in order to meet the DHS mission needs. USCIS only accesses social media content that is publicly available to all users of the social media platform to fulfill the DHS mission of enhancing national security and the integrity of the legal immigration system. Officers do not communicate with users of social media sites and only passively review information that is publicly available to all users of the social media platform. In addition, generally other than discretionary overseas denials, USCIS would not deny a benefit based on social media information without first confronting the applicant, petitioner, or benefit requestor with the information and providing an opportunity to explain it or rebut any negative inferences USCIS may have drawn from it. See 8 C.F.R. § 103.2(b)(16)(i) and (ii). USCIS requires the ability to consider this information as it may contradict or substantiate information provided by applicants in connection with an immigration

			request and for national security and public safety purposes.
1265 1271 1275 1276	Deter Travel or Immigration	**1. Chilling Effect on Expression**: Fear of government surveillance may lead applicants and their associates to self-censor, limiting their freedom of speech and association, especially regarding political or personal expression. This could deter individuals from applying for immigration benefits. **2. Deterrence from Seeking Benefits**: Fear of surveillance and privacy violations may deter crime victims, trafficking survivors, and those with complex social media histories, from applying for immigration benefits, undermining programs designed to protect them.	**Response:** DHS seeks to balance its goals of securing the U.S. border and immigration system while facilitating legitimate travel and provision of immigration benefits to eligible aliens. While we recognize that this collection may influence the decisions of a limited number of travelers or immigration benefit seekers, DHS's top priority is the safety and security of the American people and homeland. DHS does not seek to unnecessarily burden individuals but rather seeks to obtain all information necessary to maintain a robust and dynamic screening system. Comments about free speech are addressed in ***Topic 6, Constitutional issues***.
1265 1270 1271	Government Burden	The comments collectively highlight several concerns about the burden the proposed Social Media Collection would impose on the government. Key points include: **1. Administrative Burden**: Collecting and analyzing social media data is described as a misuse of government time and resources, as social media is unreliable for assessing security risks or determining immigration eligibility. Officials may spend excessive time reviewing accounts, interpreting posts, and searching for evidence, far exceeding the estimated time required. **2. Staffing Challenges**: The comments emphasize that the government lacks sufficient staff to handle the proposed collection, especially given ongoing staff reductions. Hiring additional personnel would incur significant costs, contradicting claims that the proposal would have no financial impact. **3. Redundant Information**: DHS already collects extensive data on applicants, including biometric data, travel history, employment records, and law enforcement information, which are more reliable for screening purposes. Social media data adds little value and duplicates information already accessible to DHS. **Recommendations:** • **Limit collection to relevant cases**: Only collect social media data for high-risk cases with probable cause and judicial oversight. • **Use existing data**: Rely on current DHS data sources instead of duplicating efforts. • **Restrict scope**: Collect only essential social media data tied to national security concerns.	**Response:** The addition of social media identifiers to the nine impacted forms will add a negligible amount of time to USCIS processing. The collection of social media identifiers and associated platforms will assist DHS by reducing the time needed to validate the attribution of the publicly available posted information to the individual and prevent mis-associations. It will provide trained DHS adjudication personnel with more timely visibility of the publicly available information on the platforms provided by the individual. While social media handles would be only one piece of a large mixture of information used in the analysis of eligibility for an immigration benefit, a more robust screening process may reduce unnecessary delays and costs by limiting the filing of requests for immigration benefits for or by ineligible aliens or reducing erroneous approvals that must later be addressed through revocation, rescission, or similar processes. DHS may consider any potential costs from increased social media screenings when it conducts a comprehensive fee review in the future. USCIS will continue to provide resources and training to employees to ensure comprehensive, prudent, and efficient social media screening in the future and monitor resource allocation in order to meet the DHS mission.

1271	Artificial Intelligence (AI) Concerns	**Concerns About AI Use:** **1. Bias**: AI tools may reflect biases in their training data, leading to discriminatory outcomes. **2. Context Misinterpretation**: AI struggles with slang, memes, sarcasm, and cultural nuances, increasing the risk of false positives. **3. Non-English Language Issues**: AI tools often perform poorly with non-English languages, disproportionately affecting non-citizen applicants. **4. Lack of Oversight**: DHS lacks adequate governance to ensure AI compliance with privacy, civil rights, and civil liberties. **5. Chilling Effect**: AI monitoring may pressure individuals to self-censor or limit their online activity, undermining free speech. **6. Risk to Anonymity**: AI could expose pseudonymous or anonymous users, endangering those discussing sensitive topics. **Recommendations:** **1. Improve Oversight**: Establish governance processes to ensure AI tools comply with privacy and civil rights standards. **2. Limit AI Use**: Restrict AI to targeted cases with clear security risks and avoid sole reliance on AI for decisions. **3. Improve Training**: Train officials to understand social media norms, linguistic nuances, and cultural contexts. **4. Avoid Overreach**: Reduce reliance on AI for non-English or context-sensitive social media analysis.	**Response:** Determinations for travel, entry, and immigration benefits will be made by trained DHS officers and not by computer systems or algorithms. USCIS does not use artificial intelligence for social media vetting. Trained DHS personnel may review publicly available social media information accessed via the social media identifier(s) provided by individuals as additional data points to assist in vetting of an application. Immigration benefits will be independently reviewed, and a case-by-case determination will be made by DHS officers based on the totality of the circumstances. In addition, generally other than discretionary overseas denials, USCIS would not deny a benefit based on social media information without first confronting the applicant, petitioner, or benefit requestor with the information and providing an opportunity to explain it or rebut any negative inferences USCIS may have drawn from it. See 8 C.F.R. § 103.2(b)(16)(i) and (ii).
Topic 6. Constitutional Issues			
1258 1259 1260 1261 1264 1267 1271 1273 1275 1276	First Amendment/Free Speech/Chilling Effect	The comments raise the following concerns about potential violations of the First Amendment. **1. Freedom of Speech:** The comments argue that the proposed collection of social media identifiers infringes on freedom of speech by allowing the government to monitor and potentially penalize individuals for their online expression. This includes both citizens and noncitizens, as the First Amendment protects speech and expressive conduct on social media platforms. **2. Viewpoint Discrimination:** The proposed collection is criticized for enabling immigration officers to exercise discretion in ways that could lead to viewpoint discrimination, where	**Response:** The Department respects every individual's right to maintain an opinion without interference and to seek, receive, and impart information and ideas of all kinds. The proposal to collect publicly available social media information to assist in determining admissibility or eligibility for immigration benefits is consistent with this commitment. Consistent with the requirements of the Privacy Act (5 U.S.C. § 552a(e)(7)), DHS does not maintain records "describing how any [citizen of the United States or alien lawfully admitted for permanent residence] exercises rights guaranteed by the First Amendment, unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an

		applicants might be denied immigration benefits based on speech that the government or individual officers find unfavorable. **3. Anonymity:** The comments emphasize the importance of anonymous speech, which has been historically protected under the First Amendment (e.g., Talley v. California, McIntyre v. Ohio). The proposed collection undermines this right by requiring applicants to disclose pseudonymous or anonymous social media identifiers, which could harm individuals who rely on anonymity for safety or to express dissenting views. **4. Freedom of Association:** The comments highlight that social media platforms reveal individuals' associations, connections, and affiliations, which could be subject to government scrutiny under the proposed collection. **5. Chilling Effect:** The proposed rule is criticized for creating a chilling effect on free speech, as individuals may self-censor or limit their online activity out of fear that their social media posts could be misinterpreted or used against them in immigration decisions. This fear extends to their associates and family members, further inhibiting speech and expression. The requirement to disclose social media identifiers may also further isolate vulnerable populations by discouraging them from engaging in online communities or expressing their views. **Recommendations:** **1. Rescind the Proposal**: Withdraw the proposed collection entirely. **2. Protect Anonymity**: Avoid requiring disclosure of pseudonymous or anonymous social media identifiers, which are essential for free speech, privacy, and open discourse. **3. Limit Data Sharing**: Restrict sharing of collected social media data with foreign governments, especially repressive regimes, to protect individuals from persecution or penalties. **4. Establish Clear Criteria**: Define transparent standards for what types of speech or associations may lead to adverse immigration decisions, preventing arbitrary or discriminatory enforcement. **5. Minimize Chilling Effects**: Implement safeguards to prevent self-censorship, ensuring	authorized law enforcement activity." Furthermore, DHS policy directs that "DHS personnel shall not collect, maintain in DHS systems, or use information protected by the First Amendment unless (a) an individual has expressly granted their consent for DHS to collect, maintain and use that information; (b) maintaining the record is expressly authorized by a federal statute; or (c) that information is relevant to a criminal, civil or administrative activity relating to a law DHS enforces or administers. In addition, DHS personnel should not pursue by questioning, research, or other means, information relating to how an individual exercises his or her First Amendment rights unless one or more of the same conditions applies." Details about collected data, including how USCIS uses information, shares information and protects information are provided publicly via Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs) on the DHS website. Each USCIS form also has a DHS Privacy Notice that details the authority of DHS to collect information, its purpose, when it may be disclosed, and applicable routine uses. To ensure compliance with these policies, USCIS officers must complete annual training on the operational use of social media and sign a Rules of Behavior document. Additionally, DHS will not request user passwords in furtherance of this collection and will not violate or attempt to subvert individual privacy settings or controls individuals may have implemented on social media platforms.

		individuals do not feel compelled to limit their speech or online activity out of fear of government retaliation. **6. Narrow the Scope**: Restrict the collection to publicly available information and exclude private or sensitive data irrelevant to immigration adjudication. **7. Focus on True Threats**: Limit categorization of speech as a security or public safety threat to unprotected speech, such as true threats, incitement, or fighting words.	
1260 1264 1267 1273	Fourth Amendment i. Overreach	The comments raise the following concerns about potential violations of the Fourth Amendment. Key points are below: **1. Expectation of Privacy**: The collection of social media identifiers is seen as an intrusion into individuals' private digital spaces. Many argue that social media profiles, especially those set to private, should be protected under the Fourth Amendment, which guards against unreasonable searches and seizures. **2. Applicability to Non-U.S. Citizens and U.S. Citizens:** The comments highlight that both non-U.S. citizens with substantial voluntary connections to the U.S., such as permanent residents, and U.S. citizens are entitled to Fourth Amendment protections. The proposed rule fails to account for these protections, subjecting non-U.S. citizens to potentially unconstitutional searches and implicating the privacy rights of U.S. citizens who interact with them online, which are clearly protected and subject to strict scrutiny. **3. Government Overreach:** The comments argue that the proposed collection of social media identifiers represents significant government overreach by normalizing invasive surveillance practices in the immigration process. The rule's broad and vague standards grant immigration officers excessive discretion, increasing the risk of arbitrary enforcement and undermining constitutional protections. Additionally, the collection of sensitive social media data, which reveals intimate details about individuals' lives and associations, is seen as disproportionately intrusive and unnecessary for immigration adjudication, failing to meet legal standards of necessity and practical utility. **Recommendations:** **1. Rescind the Proposal**: Withdraw the proposed collection entirely.	**Response:** DHS disagrees that the collection of social media identifiers violates the Fourth Amendment, individual expectations of privacy, or the prohibition on unlawful or warrantless searches and seizures. This collection is consistent with Supreme Court rulings related to Fourth Amendment protections to the extent such protections are applicable in this context. It is not a violation of the Fourth Amendment to ask questions of an individual who is not detained and may choose whether or not to answer them. *See, e.g., Florida v. Royer*, 460 U.S. 491, 497 (1983) (citing cases). Individuals who choose to seek admission to the United States or apply for immigration benefits do so on a voluntary basis. DHS provides ample notice that information provided by individuals may be verified and additional background checks may be conducted for the requested benefit eligibility. Additionally, federal laws, including the Immigration and Nationality Act (INA) and Homeland Security Act of 2002, and regulation provide authority for this information collection. For example, INA § 287(b), 8 U.S.C. § 1357(b), and 8 C.F.R. § 287.5(a)(2) empower officers and agents to "take and consider evidence concerning the privilege of any person to enter, reenter, pass through, or reside in the United States." Similarly, for naturalization purposes, INA § 335, 8 U.S.C. § 1446, empowers any employee of USCIS to conduct a personal investigation of the person applying for naturalization, take testimony concerning the admissibility of the applicant for naturalization, and require the production of relevant books, papers, and documents. USCIS personnel will only use social media identifiers to locate and review publicly available social media information and, as the Supreme Court has explained, "What a person knowingly exposes to the public . . . is not a subject of

		2. Require Reasonable Suspicion: Ensure that the collection of social media data is based on reasonable suspicion of involvement in a crime, as required by Fourth Amendment precedents, rather than allowing broad and arbitrary surveillance. **3. Limit Intrusions:** Restrict the scope of data collection to avoid excessive and invasive monitoring of individuals' private lives, ensuring that any intrusion is proportional and narrowly tailored to its stated purpose. **4. Address Impacts on U.S. Citizens:** Prevent the collection of information about U.S. citizens' speech, associations, and other activities on social media, as this data is clearly protected by the Fourth Amendment and First Amendment. **5. Ensure Transparency and Accountability:** Provide clear justification for the necessity of the data collection and its practical utility, and establish oversight mechanisms to prevent misuse and ensure compliance with constitutional and legal standards.	Fourth Amendment protection." *Katz v. United States*, 389 U.S. 347, 351 (1967); *see, e.g., Palmieri v. United States*, 72 F. Supp. 3d 191, 210 (D.D.C. 2014) (holding that a Plaintiff cannot claim a Fourth Amendment violation because there is "no reasonable expectation of privacy in the information [the Plaintiff] made available to 'friends' on his Facebook page"); *United States v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) ("When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment."). DHS disagrees that it should define specific criteria under which individuals may be subject to social media vetting and believes that social media screening is best applied to requests for an immigration benefit requiring a background investigation. Social media involves publicly available information that is accessible to anyone without a warrant and DHS would not be unique in reviewing it. Along with checking against government systems and information, DHS officers may use publicly available information, social media included, as part of the vetting and screening process to verify the information submitted. Moreover, the content of an individual's public social media can be used to assess and identify immigration fraud, bars to eligibility, and national security and public safety threats, requiring vetting procedures that are as broad as possible. DHS acknowledges that some of the individuals impacted will be United States citizens, however collecting social media information from U.S. citizen petitioners is within the scope of the authority of DHS. In many circumstances, the alien's relationship to a United States citizen is material to the benefit sought. The Immigration and Nationality Act (INA) authorizes DHS to collect information needed to assess eligibility for an immigration benefit. USCIS notes that the information collected will assist USCIS to evaluate other information key to benefit eligibility. In many circumstances, this will involve information from a United States citizen who has filed an immigration benefit request on behalf of an alien.
1258 1264 1271	Due Process under the Fifth and Fourteenth Amendments	The comments raise the following concerns about due process under the Fifth and Fourteenth Amendments: **1. Procedural Due Process Violations**: Comments argue that the proposed social media collection violates procedural due process by failing to provide clear, consistent, and fair standards for applicants. The lack of precise guidance on what	**Response:** DHS disagrees that collection of social media identifiers violates the individual's right to due process under both the Fifth and Fourteenth Amendments. The Supreme Court has construed the Fourteenth Amendment's Due Process Clause to impose the same due process limitations on the states as the Fifth Amendment does on the federal government. As DHS is part of the Executive Branch, and thus, the Federal

		constitutes "social media" and the broad, vague requirements for disclosure create significant barriers to compliance. Applicants may inadvertently fail to meet the requirements due to confusion or inability to recall all relevant information, leading to unjust denials of immigration benefits. **2. Discretionary Decision-Making**: Comments highlight the discretionary nature of immigration decisions, which already result in inconsistent outcomes for applicants with similar cases. Adding social media data as a factor for review exacerbates this issue, allowing immigration officers to exercise broad discretion that could lead to arbitrary or biased decisions, further undermining fairness and due process. **3. Responsibility for Third-Party Compliance**: Imposes an undue burden on applicants by requiring them to solicit sensitive social media information from third parties, such as relatives or minor children. This creates additional challenges, as third parties may withhold information, fail to recall identifiers, or misunderstand the requirements. Such dependency on third-party compliance could result in unfair denials of immigration benefits, violating due process protections. **4. Risk of Pretextual Denials**: The vague and sweeping language of the rule increases the risk of pretextual denials, where applicants could be rejected for minor or inadvertent errors, long-forgotten identifiers, or subjective interpretations of their social media activity. This undermines the fairness and transparency required by due process. **5. Substantive Due Process Violations**: Comments emphasize that due process protects against the unfair deprivation of substantive rights, such as free expression and access to non-discretionary immigration relief (e.g., naturalization). The proposed collection could lead to the denial of these rights based on arbitrary or discriminatory factors, further violating due process principles. **Recommendations:** **1. Rescind the Proposal**: Withdraw the proposed collection entirely. **2. Provide Clear Standards and Definitions**: Establish precise definitions for terms like "social media" and "social media identifiers" to eliminate vagueness. Clearly define what constitutes a security or public safety threat. DHS	Government, it is not clear how the Fourteenth Amendment is applicable in this instance. Regarding the Fifth Amendment, the proposed information collection does not impact the due process rights of applicants, petitioners, or benefit requestors. For example, in general other than discretionary overseas denials, USCIS would not deny a benefit based on social media information without first confronting the applicant, petitioner, or benefit requestor with the information and providing an opportunity to explain it or rebut any negative inferences USCIS may have drawn from it. See 8 C.F.R. § 103.2(b)(16)(i) and (ii). Additionally, if USCIS makes an adverse finding on any request or application, the individual may be entitled to additional immigration processes which may include the right to appeal or appear before an immigration judge. Regarding third-party compliance, DHS notes that in most cases, we are only requesting social media regarding about the applicant, beneficiary, or petitioner. We will not request social media information for every relative nor family member. In some specific cases, social media information will be requested only from family members with direct ties to the petition itself and/or the benefit requested. For more information about the clear standards and definitions that DHS has provided for social media terms, please see ***Topic 8. Unreliable Information****, Imprecise/Confusing Social Media Terms.*

		must provide detailed and transparent instructions to ensure applicants can comply with the proposed collection without inadvertent errors or omissions. **3. Restrict Officer Discretion**: Implement strict guidelines to limit immigration officers' discretion in interpreting social media information. **4. Exclude Third-Party Information:** Applicants should not be required to disclose social media identifiers for relatives, minor children, or other third parties, as this places an undue burden on applicants and risks violations of privacy and fairness. **5. Prevent Pretextual Denials**: Explicitly prohibit the use of minor errors, omissions, or subjective interpretations of social media activity as grounds for denying immigration benefits or stripping applicants of their status.	
1264 1273	Fifth Amendment – Self Incrimination	The comments raise the following concerns about the Fifth Amendment and self-incrimination: **1. Compelled Disclosure of Private Information**: The proposed rule requiring applicants to disclose social media identifiers, including pseudonymous or anonymous accounts, is described as a form of compelled disclosure that could force individuals to reveal private information. This compelled disclosure may lead to self-incrimination, as applicants could be required to provide information that might be used against them in immigration decisions. **2. Risk of Pretextual Denials**: The comments highlight the risk of pretextual denials of immigration benefits based on minor or inadvertent omissions, forgotten social media identifiers, or associations with disfavored individuals or groups. Applicants could be unfairly penalized for providing incomplete or inaccurate information, raising concerns about self-incrimination and the potential misuse of their disclosures. **3. Guilt by Association**: The rule's focus on collecting social media identifiers could result in applicants being held accountable for their associations or interactions with others online, even if those associations are innocuous or unrelated to the applicant's eligibility. This raises concerns about individuals being indirectly incriminated through their social media connections, violating the Fifth Amendment's protection against self-incrimination.	**Response:** The Fifth Amendment prohibition against self-incrimination applies to proceedings in which the Government seeks to compel testimony that a witness reasonably believes could be used against him in a state or federal criminal proceeding. A risk that the testimony might subject the witness to deportation or other civil consequences (such as, here, denial of an immigration benefit) is not a sufficient ground for asserting the privilege. *See United States v. Balsys*, 524 U.S. 666, 671–72 (1998). Additionally, here, the Government does not seek to compel testimony, but rather plans to collect publicly available social media information already posted by an individual. Despite the inapplicability of the Fifth Amendment in this situation, DHS is not requiring individuals to incriminate themselves by providing social media identifiers to USCIS on its forms. Filing for immigration benefits and including requested information is a voluntary action by an individual. Information about the use of provided information by the government is explained in SORNs, PIAs and the DHS Privacy Notice provided on every USCIS form.

		4. Chilling Effect on Speech and Associations: The fear of being required to disclose social media activity and associations may lead applicants to self-censor, delete posts, or avoid certain platforms altogether. This preemptive self-censorship reflects the broader concern that individuals may feel forced to alter their behavior to avoid providing incriminating information. **Recommendations:** **1. Establish Clear Standards**: Define key terms and provide strict guidelines to limit officer discretion, ensure fair decision-making, and prevent arbitrary enforcement. **2. Protect Privacy and Anonymity**: Safeguard the right to anonymous speech, implement strict data retention and sharing protocols, and conduct privacy impact assessments to mitigate risks, especially for vulnerable populations. **3. Clarify Compliance Requirements**: Provide clear instructions to prevent inadvertent errors and ensure applicants can meet the rule's requirements without undue burden.	
Topic 7. Public Safety			
1261 1269 1274 1275 1276	Discriminatory/Safety Risk	The comments provided raise significant concerns about discrimination and safety risks associated with the proposed collection of social media identifiers. Below are the key points: **Discrimination Concerns:** **1. Bias in Decision-Making:** The collection of social media data risks introducing subjective biases into immigration adjudications, as reviewing officers may interpret social media activity based on their personal views rather than objective criteria. **2. Targeting Marginalized Groups**: The collected data could be misused to target individuals based on their race, ethnicity, political views, or associations, amplifying systemic inequities. Historical examples of surveillance disproportionately targeting Black and Latinx communities, political activists, and immigrants are cited to highlight how broad discretion in data collection could perpetuate systemic discrimination. **3. Guilt by Association**: Comments emphasize the risk of applicants being penalized for their associations or interactions on social media, even if they are tenuous or misinterpreted. **Safety Risks:**	**Response:** DHS is steadfastly committed to the highest standards of conduct, especially when it comes to the fair, unbiased, and transparent enforcement of our mission responsibilities. The collection of this additional information will be used to help enforce our immigration laws by assisting in the adjudication of eligibility to be admitted to the United States or be granted an immigration-related benefit. Existing DHS policy prohibits the consideration of race or ethnicity in our investigation, screening, and enforcement activities in all but the most exceptional instances. This policy is reaffirmed in manuals, policies, directives, and guidelines. Existing DHS policy also prohibits profiling, targeting, or discrimination against any individual for exercising his or her First Amendment rights. We will not use the information in a discriminatory manner that prevents entry into the United States or denies benefits based on an individual's race, color, age, sexual orientation, religion, sex, national origin, or disability. DHS will handle social media identifiers in the same manner as other information collected for immigration benefit purposes. Social media information is one data point for benefit requesters and is intended to be considered along with other information, including other application data provided by individuals. DHS will make case-by-case determinations based on the

		1. Victim Retraumatization: Requiring crime victims and trafficking survivors to disclose social media accounts risks retraumatizing them echoing lack of privacy and enabling perpetrators to further exploit or falsely accuse them. **2. Weaponization of Social Media by Perpetrators**: Traffickers and abusers often use social media to manipulate, monitor, or harm their victims. The proposed rule could inadvertently amplify these risks by requiring victims to disclose accounts that may have been compromised or controlled by their abusers. **Conclusion:** These concerns suggest that the rule may harm vulnerable populations and fail to achieve its stated objectives of improving national security and public safety.	totality of the circumstances. In addition, generally other than discretionary overseas denials, USCIS would not deny a benefit based on social media information without first confronting the applicant, petitioner, or benefit requestor with the information and providing an opportunity to explain it or rebut any negative inferences USCIS may have drawn from it. See 8 C.F.R. § 103.2(b)(16)(i) and (ii). DHS disagrees with commenters who believe victims of crime and trafficking will be traumatized by providing social media information. The information is neither substantive nor detailed, and does not contain account content. Any information provided by an individual on a form is done so voluntarily by the individual. DHS does not compel individuals to request immigration benefits from USCIS. Officers who conduct social media evaluations are trained to identify accounts potentially controlled by someone other than the applicant, petitioner, or beneficiary. In the event that an applicant, petitioner, or beneficiary's account had been compromised by another individual, USCIS generally would not deny a benefit based on any negative inference without first confronting the applicant, petitioner, or beneficiary with the information and providing an opportunity to explain the circumstances around any compromised social media account or rebut any negative inferences USCIS may have drawn from it. See 8 C.F.R. § 103.2(b)(16)(i) and (ii). USCIS complies with the Privacy Act and DHS policy regarding collection and protection of information as required. DHS understands that information provided on its forms may be about U.S. citizens and lawful permanent residents who are covered by the Privacy Act, and DHS employees, who are permitted and trained to utilize social media for operational purposes during the performance of their duties, must adhere to DHS privacy policies, as established by the Chief Privacy Officer. Furthermore, USCIS follows all applicable laws, regulations and policies to protect collected information and use it for its designated purpose. DHS provides public notice about collection and use of data under appropriate System of Records Notices (SORNs) published online and in the Federal Register, Privacy Impact Assessments (PIAs) posted on the DHS website, and privacy

			notices on DHS forms. DHS has evaluated potential privacy risks and determined that multiple published System of Record Notices (SORNs) in the Federal Register and associated Privacy Impact Assessments (PIAs) cover and apply to information gathered in this collection.
Topic 8. Unreliable Information			
1263 1264 1268 1273 1275	Imprecise/Confusing Social Media terms	The comments highlight several issues regarding the imprecision, confusion, and potential unreliability of collecting social media information. Key points include: **Imprecision and Vagueness** **1. Undefined Terms**: The lack of clear definitions for terms like "social media identifier" or "platform" creates confusion for applicants. Without a concrete list of platforms or specific guidance, applicants are left to guess what information is required. **2. Overbroad Scope**: The requirement to list all social media accounts used over the past five years is seen as excessively broad, encompassing platforms that may not be relevant to immigration adjudication. **Recommendations:** **1. Withdraw the Proposal**: Many commenters recommend rescinding the proposed collection entirely, as it is seen as unnecessary, overly burdensome, and prone to generating unreliable data. **2. Provide Clear Definitions**: If implemented, the proposed collection should narrowly define what constitutes a "social media identifier" and limit the scope to current, verifiable accounts. Offer a definitive list of social media platforms that applicants must disclose, reducing ambiguity about what is expected. **3. Limit Scope**: Avoid requiring identifiers for platforms unrelated to immigration adjudication, such as shopping sites, hobby forums, or niche platforms.	**Response:** DHS defines social media as the "sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact." Social media platforms include Facebook, X (formerly Twitter), Instagram, among others, that are commonly identified as "social media". That definition has been used by DHS previously. Please see the Privacy Impact Assessment found at https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-013-01-fdns-august2019.pdf. This definition of "social media," as well as a list of examples of social media platforms, is specifically included in the form instructions for each of the forms collecting social media information, and DHS expects the definition and examples to eliminate any confusion concerning the definition of a "social media platform." DHS believes the term "social media identifier" is sufficiently descriptive and will be commonly understood by the public to signify one's "username", "ID", or "handle". Based on our research, we think the terms used and the additional information in form instructions are sufficient, but we welcome public comments on additional terms that we should consider. If a social media platform does not use a handle, the new form instructions request that individuals provide the relevant associated identifiable information used to access the platform, such as an email address or phone number.
1263 1264 1268 1273 1275	No Social Media Presence/False Information	The comments highlight several concerns about how the collection of social media information may lead to unreliable data due to a lack of social media presence or the prevalence of false information. Key points include: **1. Lack of Social Media Presence** • **No Social Media Accounts**: Not all applicants have a social media presence, and some may intentionally avoid using social media platforms for privacy or personal reasons. This could lead to	**Response:** DHS has a layered approach to security and any social media identifiers collected would be only one piece of information used in the analysis of eligibility for the requested immigration benefit. Although the potential exists for an individual to provide false or inaccurate information about their social media identifiers on a form, the response (or lack thereof) the individual provides in the context of the larger picture will guide the line of inquiry pursued by the DHS officer. The potential for inaccurate/false social media or other

		unfair assumptions about their eligibility or intent. **2. Forgotten or Inactive Accounts:** • **Forgotten Accounts**: Many applicants may struggle to recall all the accounts, usernames, or pseudonyms they've used over the past five years, especially for inactive or forgotten accounts. • **Multiple Accounts**: Applicants often have multiple accounts on the same platform due to forgotten passwords or different purposes, making it challenging to provide a complete and accurate list. • **Unintentional Omissions**: Forgetting to disclose an account, even unintentionally, could lead to accusations of misrepresentation, creating a "trap" for applicants. **3. Prevalence of False Information** • **Fake Accounts**: Social media platforms do not require identity verification, making it easy for individuals to create fake or spoofed accounts. This undermines the reliability of social media data for identity verification or security screening. • **Manipulated Content**: Social media posts can be edited, fabricated, or taken out of context, leading to false conclusions about an applicant's character or intent. • **Unverifiable Data**: Many social media identifiers are pseudonymous or auto-generated, making it difficult for adjudicators to verify the authenticity of the information provided. **Recommendations:** **1. Focus on Current Accounts**: Focus on current, verifiable accounts and exclude inactive or irrelevant platforms to minimize the risk of unreliable data. **2. Adopt a Targeted Approach**: Reserve social media reviews for cases with specific, articulable risk indicators rather than applying the requirement universally. **3. Cross-Check Data:** Implement safeguards to verify the authenticity of social media information before using it as a basis for decisions. **4. Avoid Penalizing Omissions**: Ensure that unintentional omissions or forgotten accounts do	application information does not render the collection of this information unnecessary. DHS makes case-by-case determinations based on the totality of the circumstances consistent with its authorities. In addition, generally other than discretionary overseas denials, USCIS would not deny a benefit based on social media information without first confronting the applicant, petitioner, or benefit requestor with the information and providing an opportunity to explain it or rebut any negative inferences USCIS may have drawn from it. See 8 C.F.R. § 103.2(b)(16)(i) and (ii). DHS is aware that some individuals may not have social media accounts, therefore USCIS has updated the proposed collection of information to include the following question on each impacted information collection: "Have you had or used a social media account in the past five (5) years? Yes/No." Collection of social media information will not be used for identity verification. Social media may be used to support or corroborate application information, which will help USCIS' mission to administer the nation's lawful immigration system by providing an additional means to adjudicate issues related to relevant questions about identity, occupation, previous travel, and other factors. It may also be used to identify potential deception or fraud.

		not result in accusations of misrepresentation or denial of benefits.	
1264 1265 1273	Language Concerns	The comments raise concerns about language regarding the proposed collection of social media identifiers. • **Language Differences**: Social media posts in languages other than English may be mistranslated or misunderstood, leading to incorrect conclusions about an applicant's intent or character. **Recommendations:** • **Cultural and Linguistic Training**: Ensure adjudicators are trained to interpret social media posts in different languages and cultural contexts to avoid misinterpretation.	**Response:** DHS officers and personnel have extensive background in reviewing documentation in languages other than English, and they are trained to consider linguistic and cultural nuance. The addition of social media vetting would not be unique to DHS investigative and adjudicative practices with respect to sources and documentation in foreign languages. If derogatory information in a foreign language were found in social media, USCIS generally would not deny a benefit based on such information without first confronting the applicant, petitioner, or benefit requestor with the information and providing an opportunity to explain it or rebut any negative inferences USCIS may have drawn from it. See 8 C.F.R. § 103.2(b)(16)(i) and (ii). Individuals may also submit a full and complete English language translation of foreign language social media documentation in response to a USCIS notice or request . The translator must certify that the translation is accurate, and he or she is competent to translate from that language to English.
Topic 9. Public Concerns Expressed			
1266 1269	General Opposition	The comments broadly oppose the proposed collection of social media identifiers, arguing that it infringes on free speech, fosters unconstitutional viewpoint discrimination, and perpetuates xenophobic policies. Commenters expressed concern that the collection would limit immigrants, tourists, and legal residents from engaging in protected speech, particularly when criticizing the government or discussing sensitive topics like U.S. foreign policy. The policy is described as part of a broader agenda to enable mass deportations with reduced legal standards, undermining constitutional protections. Additionally, commenters highlight the misallocation of government resources, suggesting that time spent on social media monitoring could be better used addressing issues like unlawful detentions. The proposal is seen as creating a chilling effect, where individuals may self-censor to avoid adverse immigration consequences, ultimately harming democratic principles and open discourse. Overall, the comments argue that the rule is unnecessary, discriminatory, and counterproductive to legitimate administrative and national security goals.	**Response:** Two commenters did not make clear objections. Therefore, DHS cannot provide specific responses to these general oppositions. DHS's role in reviewing publicly available social media information accessed via social media identifier(s) provided by individuals is appropriate given that DHS's mission to is to secure the Nation from threats. This includes denying immigration benefits to inadmissible or ineligible aliens, as appropriate and in accordance with law, including criminals and terrorists. USCIS officers make their decisions based on the requirements of U.S. immigration law and DHS policies. Information found on social media via the provision of social media identifier(s) will enhance the vetting process and identify potential threats. For example, social media may be used to support or corroborate a benefit seeker's application by providing an additional means to adjudicate issues related to relevant questions about identity, occupation, previous travel, and other factors. It may also be used to identify potential deception or fraud. Social media may help distinguish individuals of additional concern from those individuals whose information substantiates their eligibility for immigration benefits.

1271 1273	Excessive Government Oversight	The comments highlight that the proposed collection of social media identifiers allows for excessive government oversight by enabling indefinite monitoring and broad data sharing with minimal transparency or safeguards. DHS's retention and dissemination policies would permit ongoing surveillance of individuals, including U.S. citizens, and the sharing of sensitive data with domestic and international entities, potentially exposing individuals to harm or persecution. Weak oversight mechanisms and a lack of clear rules or privacy protections further exacerbate the risks of civil liberties violations and data breaches. This unchecked oversight is seen as disproportionate, unnecessary, and harmful to privacy and free expression.	**Response:** Individuals who present a threat to national security or public safety are not eligible for certain benefits and U.S. immigration laws preclude DHS from granting immigration and naturalization benefits to individuals with certain disqualifying characteristics including association with terrorist organizations. See, e.g., INA § 208(b)(2)(A), 8 U.S.C. § 1158(b)(2)(A) (mandatory bars to asylum); INA § 245(a)(2), 8 U.S.C. § 1255(a)(2) (admissibility requirements for adjustment of status applicants and agency discretion); and INA § 316(a)(3), 8 U.S.C. § 1427(a)(3) (good moral character requirement for naturalization). Investigation of social media activity will assist USCIS in making sure that these requirements are met. As noted in prior responses, USCIS collects information from individuals voluntarily applying for immigration benefits. USCIS follows all applicable laws, regulations and policies to protect collected information and use it for its designated purpose. Furthermore, as noted in a prior response, Officers who are responsible for conducting social media vetting are trained specifically on how to identify First Amendment activity. USCIS has extensively detailed the process for social media vetting publicly via the Privacy Impact Assessment (PIA) in 2019: https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-013-01-fdns-august2019.pdf.
Topic 10. Out of Scope			
1262		There was one comment received that is out of scope.	**Response:** DHS did not address this comment because it was outside the scope of the proposed generic clearance.