Rules and Regulations

Federal Register
Vol. 75, No. 162
Monday, August 23, 2010

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS–2010–0054]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/United States Citizenship and Immigration Services—009 Compliance Tracking and Management System of Records

AGENCY: Privacy Office, DHS.

ACTION: Final rule.

SUMMARY: The Department of Homeland Security is issuing a final rule to amend its regulations to exempt portions of a Department of Homeland Security/United States Citizenship and Immigration system of records entitled the "United States Citizenship and Immigration Services—009 Compliance Tracking and Management System of Records" from certain provisions of the Privacy Act. Specifically, the Department proposes to exempt portions of the Department of Homeland Security/United States Citizenship and Immigration Services—009 Compliance Tracking and Management System of Records from certain provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: This final rule is effective August 23, 2010.

FOR FURTHER INFORMATION CONTACT: For general questions please contact Monitoring and Compliance Branch Chief (202–358–7777), Verification Division, U.S. Citizenship and Immigration Services, Department of Homeland Security, 470 L'Enfant Plaza East, SW., Suite 8204, Washington, DC 20529. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

Background

The Department of Homeland Security (DHS) published a notice of proposed rulemaking (NPRM) in the **Federal Register,** 74 FR 23957, May 22, 2009, proposing to exempt portions of the DHS/United States Citizenship and Immigration Services (USCIS)—009 Compliance Tracking and Management System (CTMS) of Records from certain provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. The DHS/USCIS—009 Compliance Tracking and Management system of records notice (SORN) was published concurrently in the **Federal Register**, 74 FR 24022, May 22, 2009 and comments were invited on both the NPRM and SORN. Comments were received on both the NPRM and SORN.

Comments on the Notice of Proposed Rulemaking (74 FR 23957, May 27, 2009)

DHS/USCIS received seven comments on the NPRM (74 FR 23957, May 22, 2009) and twelve on the SORN (74 FR 24022, May 22, 2009). One set of comments relates to a potential operational concern with the SAVE program that pertains to the DHS/USCIS—004 Verification Information System (VIS). While CTMS does deal with SAVE data, the comments in question did not relate to compliance and monitoring issues. These comments are being addressed by the SAVE program. Another set of comments concerned corporate hiring practices and did not relate to CTMS or compliance and monitoring issues generally.

Below is an analysis of each comment that specifically relate to this NPRM that is not addressed directly above. Comments were received from the National Immigration Law Center (NILC) regarding several elements of the CTMS SORN and corresponding Notice of Proposed Rulemaking (NPRM)

Comment: NILC stated that law enforcement exemptions were overbroad and unwarranted.

Response: The Department notes that Congress has stated its understanding that the USCIS employment verification system may be used for law enforcement purposes when necessary to prevent violations of the Immigration and Nationality Act (INA), and in cases of document fraud, counterfeiting and perjury (8 U.S.C. 1324a(d)(2)(F)). E-Verify was originally established for the purpose of serving as a "confirmation system through which [DHS]—

(1) Responds to inquiries made by electing persons and other entities [* * *] at any time through a toll-free telephone line or other toll-free electronic media concerning an individual's identity and whether the individual is authorized to be employed, and

(2) Maintains records of the inquiries that were made, of confirmations provided (or not provided), and of the codes provided to inquirers as evidence of their compliance with their obligations under the pilot programs.". (8 U.S.C. 1324a note (at § 404(a)) "The confirmation system shall be designed and operated—

(1) To maximize its reliability and ease of use by persons and other entities making elections under section 402(a) of this division consistent with insulating and protecting the privacy and security of the underlying information;

(2) To respond to all inquiries made by such persons and entities on whether individuals are authorized to be employed and to register all times when such inquiries are not received;

(3) With appropriate administrative, technical, and physical safeguards to prevent unauthorized disclosure of personal information; and

(4) To have reasonable safeguards against the system's resulting in unlawful discriminatory practices based on national origin or citizenship status, including—

(A) The selective or unauthorized use of the system to verify eligibility;

(B) The use of the system prior to an offer of employment; or

(C) The exclusion of certain individuals from consideration for employment as a result of a perceived likelihood that additional verification will be required, beyond what is required for most job applicants.". (8 U.S.C. 1324a note (at § 404(d))

CTMS serves as a vehicle by which USCIS can comply with its statutory mandate to ensure the integrity of the verification system as outlined above. Information in CTMS may provide

evidence of the improper use of the E-Verify system which directly supports the statutory mandate to prevent the misuse, discriminatory or fraudulent use of the system. Furthermore, every request for access to information in CTMS will be evaluated with the predisposition to releasing the information. USCIS will only claim the exemption if it determines that releasing the information would be contrary to a law enforcement purpose.

Comments were received from the American Immigration Lawyer Association (AILA) regarding several points.

Comment: AILA objected to the 30-day comment period.

Response: The Department notes that the Administrative Procedure Act ("APA"), 5 U.S.C. 553(c), provides that "each agency that maintains a system of records shall at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the notice in the **Federal Register** any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency." In the absence of a demonstration of a compelling need to extend this period, such as numerous requests for additional time or when the subject of the proposed governmental action is complex or exceedingly controversial, the 30 days provided for under the APA provides an opportunity for thorough, well-informed rulemaking. While AILA's comments were the only comments submitted past the 30-day time period, USCIS did consider their comments. Based on the public comments received thus far, there is nothing to suggest that there was a need for additional time.

Comment: AILA commented that the use of CTMS for law enforcement support is contrary to Congressional intent.

Response: Congress has stated its understanding that the USCIS employment verification system may be used for law enforcement purposes when necessary to prevent violations of the INA, and in cases of document fraud, counterfeiting, and perjury in the INA 8 U.S.C. 1324a(d)(2)(F). 8 U.S.C. 1324a note (at § 404(d)) requires that E-Verify have "reasonable safeguards against the system resulting in unlawful discriminatory practices based on national origin or citizenship status, including—(A) The selective or unauthorized use of the system to verify eligibility; (B) the use of the system prior to an offer of employment; or (C) the exclusion of certain individuals from consideration for employment as a result of a perceived likelihood."

CTMS serves as a vehicle by which USCIS can comply with its statutory mandate to ensure the integrity of the verification system by preventing the fraudulent use of E-Verify and SAVE and violation of the INA, as well as any misuse or discriminatory use of the system (8 U.S.C. 1324a note (at § 404(d))).

Comment: AILA expressed concern that because E-Verify is only a pilot, any results from the system should be used only for education and outreach, not law enforcement purposes.

Response: The Department acknowledges that as long as E-Verify is operational, there is the potential that it will be misused or abused. The monitoring and compliance functionality has been established to identify and resolve noncompliance. This is particularly important, regardless of the programs' status as a pilot, where misuse of the system has an immediate effect on a person's ability to work. CTMS is an integral component of these monitoring and compliance activities, as it allows for compliance activity management and storage of the information supporting the compliance determinations surrounding use of the program.

Comment: AILA expressed concern that CTMS is not an effective way to reduce identity theft, and recommends that all multiple uses of A-Number or SSN should result in a Tentative Non-Confirmation (TNC) rather than additional further research into the employer.

Response: The Department is aware of the potential for fraudulently used identity documents to be verified through the system. The USCIS Verification Division, the component of DHS responsible for the E-Verify Program and CTMS, meets with AILA annually. During a meeting held May 7, 2009, AILA and representatives from the Verification Division discussed the monitoring of multiple SSNs. USCIS is researching solutions to this potential problem. However, multiple uses of A-Number or SSN identifications do not warrant automatic TNCs since it is feasible for one individual to be accurately verified in the system multiple times, where they may hold multiple jobs or change jobs frequently. Hence, multiple uses of an A-Number or SSN are not necessarily fraudulent and should not result in a TNC in all cases. In fact, the inconvenience that would be caused to individuals who are rightly verified multiple times would outweigh the benefit of automatic TNCs. CTMS would be used to determine under which circumstances such incidents of multiple uses would indicate a need for further compliance research and would be the tool to manage any resulting compliance activity.

Comment: AILA expressed concern that an employer might try to protect itself from law enforcement activities by only selecting employees the employer perceives to be without any potential for immigration-related violations, thereby increasing immigration-related discrimination.

Response: The Department agrees that E-Verify users may try to insulate themselves from law enforcement activities by discriminatory use of these systems. As the Department has already developed a relationship for forwarding potential violations to the Department of Justice (DOJ) Office of Special Counsel (OSC) as required by law, it is vital that the monitoring and compliance activities be well developed and managed to ensure that E-Verify is looking carefully at these issues.

Comment: AILA suggested that there are better methods for reducing discrimination and misuse of E-Verify including: (1) Improving posters and providing alternative means of notification; (2) involving OSC more directly in E-Verify education and outreach efforts; (3) modifying E-Verify case resolution functionality; (4) enhancing E-Verify user reports; and (5) providing better training and reporting tools to corporate and program administrators.

Response: The Department agrees that there should be an ongoing process of evaluating and improving the methods that are used to prevent and detect misuse. In fact, AILA's suggestion regarding improving posters is supported by the compliance activity of determining whether the posters are actually being used by employers. The development of the USCIS Verification Division Monitoring and Compliance Branch and the appropriate use of the CTMS tracking and managing tool are central to this ongoing initiative, and will be used in conjunction with other program enhancements to involve employers in the compliance assistance elements of E-Verify. In addition, E-Verify continuously evaluates and improves the means of educating users about the correct way to use E-Verify, and of informing the individuals being verified of their rights. E-Verify works closely with OSC, as appropriate, using the CTMS to guide referrals to the appropriate enforcement agency. Recent changes have included significant enhancements to the training processes and additional means of notification, including adding privacy information

on the E-Verify Web site. The Department is currently evaluating the E-Verify case resolution functionality, determining additional ways to involve the users in the integrity of the programs and is investigating enhancements to the program's reporting capabilities, to address user's ability to evaluate and train individual users, and to use other means to assist users in the E-Verify processes. Further, USCIS signed a Memorandum of Agreement with the Department of Justice's Office of Special Counsel (OSC) for Unfair Immigration-Related Employment practices on March 17, 2010 that formally establishes the relationship and process for referrals between the agencies, and continued collaboration efforts, including E-Verify education and outreach.

Comments on the System of Records Notice (74 FR 24022, May 22, 2009)

Comment: NILC expressed concern that the CTMS SORN does not adequately address how monitoring and compliance will be conducted given the expanded use of SAVE by States and localities.

Response: The Department acknowledges that the expanded use of SAVE, as required by section 642(c) of the Illegal Immigration Reform and Immigrant Responsibility Act (Pub. L. 104–208, 110 Stat. 3009), will increase the number and types of SAVE users. These users will pose different monitoring and compliance challenges. However, all SAVE user agencies are subject to the policies and procedures governing use of the system. The Department is aligning the SAVE monitoring and compliance activities with the various agencies, whether federal, state, or local, in order to identify non-compliant behaviors regardless of the specific purpose of the SAVE query. In fact, in the vast majority of cases, the same type of SAVE query is conducted using the same information and documentation regardless of the purpose of the query. CTMS will be used to track and manage these monitoring and compliance activities and provide support for SAVE monitoring and compliance deliberative processes.

Comment: NILC expressed concern that E-Verify focusing on an employer's election not to use E-Verify after registering for the program would be a waste of resources as it does not actually indicate misuse of the system.

Response: The Department appreciates NILC concern that E-Verify not waste resources on a behavior that does not indicate a misuse of the system. However, once enrolled in E-Verify, employers are required to either verify all new hires through the system, or withdraw from E-Verify. This is required in order to minimize the potential of an employer using the system in a potentially discriminatory manner by verifying some employees but not others. The Department also notes that this is a good example of a misuse that would be resolved in almost all cases by E-Verify providing compliance assistance to employers to help them understand what their responsibilities are. Although CTMS is used for identifying potentially illegal activities, compliance activities are primarily focused on education, training, and awareness to assist employers to better understand the purpose of E-Verify and their role in the process.

Comment: NILC expressed concerns that, despite DHS' stated intentions, CTMS is designed to investigate immigration offenses by employees rather than misuse by employers.

Response: The Department understands the NILC's concern, but in both the SAVE and E-Verify programs the Department is mandated to focus on the relationship with the agency or employer in its operational activities not on the applicant or employee being verified. Employers are the direct users of E-Verify as are SAVE agencies the direct users of SAVE, and it is with E-Verify employers and SAVE agencies that the E-Verify or SAVE Memoranda of Understandings (MOUs) are signed. The subject of E-Verify or SAVE verification would only be contacted if the compliance activity is based on a specific lead or tip first provided voluntarily to DHS by that subject. However, if in the course of research USCIS discovers evidence of fraud by an individual verified by SAVE or E-Verify, USCIS will evaluate those matters and may refer them to the appropriate law enforcement agency.

Comment: NILC expressed concern that if CTMS is used for immigration enforcement and Privacy Act exemptions are granted, employees, those most likely to be able to witness and report on misuse, will be unwilling to make such reports.

Response: Employee information is vital to compliance analysts for interpreting various user behaviors and the monitoring and compliance effort is essential to protecting the rights of the employee from abuse by employers and other employees, as well as determining if employer or agency users are in compliance with the program terms of use. Currently, as required by law, E-Verify forwards information that suggests illegal activities to appropriate law enforcement organizations. The Department acknowledges the risk that some employees may be unwilling to report cases of misuse of E-Verify or SAVE because of their concerns regarding CTMS's immigration enforcement capability and its Privacy Act exemptions. This risk however, is one that must be accepted in order to effectively and adequately protect the integrity of any law enforcement investigations that result from monitoring and compliance activities within CTMS.

Comments were received from the American Council on International Personnel (ACIP) regarding two points.

Comment: ACIP requested that E-Verify should work directly with employers before any effort is made to refer potential issues to law enforcement organizations.

Response: The Department agrees with ACIP and E-Verify has developed an escalating approach to compliance in which noncompliance is resolved by contacting and working with the employer directly when possible. The purpose of collecting information in the CTMS is to allow compliance analysts to determine the correct approach to involving the employer or agency in the compliance process. E-Verify begins from a position of "compliance assistance," which is to educate employers and ensure proper policies and procedures are followed. If, after the employer has been contacted, noncompliance is ongoing or more egregious, E-Verify may escalate to compliance activities that involve more direct interaction with employers, which may include collecting additional information from the employer for analysis. For those situations where USCIS believes there is more egregious noncompliance, E-Verify may make a referral to a law enforcement agency for the appropriate enforcement action. CTMS tracks and manages this process.

Comment: ACIP suggested the use of additional advanced technologies to prevent fraud and misuse.

Response: The Department appreciates ACIP's comment and is continuing to investigate a number of technologies and processes that would increase the integrity of the SAVE and E-Verify program, but believes that as no technology will be able to stop all cases of misuse, DHS must develop a system and process for researching, tracking, and managing potential cases of misuse, abuse, fraud, or discrimination.

Comment: AILA expressed concern that CTMS is beyond the scope of authority for E-Verify established by IIRIRA, but that if CTMS is to be used it should be used as a tool to focus

attention on employees who might be misusing documentation.

Response: The Department is aware of the need to ensure that that E-Verify and SAVE are not misused. However, because these programs work directly with the employers and SAVE agencies, and do not have a direct relationship with the individuals being verified, it is necessary to focus on the users of the programs. Thus, the employers and SAVE agency users create a contractual relationship with DHS through their registration and signing of the program Memoranda of Understanding (MOUs) which establish the parameters of their use. In light of this relationship, the Department can work to train users on the correct use of the programs. Until Congress directs otherwise, these programs must focus on the E-Verify and SAVE users.

Comment: AILA expressed concern that DHS failed to consult with employer representatives in the development and implementation of E-Verify as required by IIRIRA, Section 402(d)(1).

Response: E-Verify works with the user population on changes to continuously improve the program, through outreach and interaction with employers and agencies by conducting training sessions, Webinars, and outreach events throughout the United States. These outreach initiatives have resulted in changes to E-Verify, for example changes have been made to simplify E-Verify language and to change data handling procedures to make it more convenient for employers and employees using E-Verify. E-Verify also evaluates and implements, where possible, the suggestions of employer advocacy organizations, for example the program is currently evaluating changes to the program that would increase enhanced program authentication methods. The Westat Reports, the statutorily mandated third party review of E-Verify, are published to the Web to inform employers of recommendations for improving the integrity of the program. These efforts meet the requirements of IIRIRA § 402 (d)(1) which provide that DHS "shall closely consult with representatives of employers (and recruiters and referrers) in the development and implementation of the pilot programs, including the education of employers (and recruiters and referrers) about such programs."

Comment: AILA recommended that DHS not devote resources to the CTMS system until release of the pending Westat Report.

Response: The Westat Reports of 2002 and 2007 recommended that USCIS develop monitoring and compliance capability. The USCIS Verification Division Monitoring and Compliance Branch has developed CTMS as a support tool for its operations. Recommendations from the next Westat Report, along with experience from monitoring and compliance activities, will be an input to this continuous improvement function.

USCIS Verification Division Monitoring and Compliance Branch operations have been developed based on best practices, as well as knowledge of the E-Verify system and the ways in which it could potentially be misused or abused. The previous Westat Reports served as a reference while the USCIS Verification Division Monitoring and Compliance Branch was being formulated; future Westat Reports will likewise be leveraged. However, the absence of a "perfect" E-Verify system should not preclude the establishment of a monitoring and compliance component, along with the associated tools, such as CTMS. As long as the system is being used, USCIS has a responsibility to ensure that the system is being used appropriately and in accordance with program rules and regulations. The USCIS Verification Division Monitoring and Compliance Branch, and associated management tools, fulfill that function.

Having taken into consideration and addressed public comments resulting from this NPRM and SORN, as well as the Department's position on these public comments, DHS will implement the rulemaking as proposed.

List of Subjects in 6 CFR Part 5

Freedom of information; Privacy.

■ For the reasons stated in the preamble, DHS amends Chapter I of Title 6, Code of Federal Regulations, as follows:

PART 5—DISCLOSURE OF RECORDS AND INFORMATION

■ 1. The authority citation for Part 5 continues to read as follows:

Authority: Pub. L. 107–296, 116 Stat. 2135, 6 U.S.C. 101 et seq.; 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

■ 2. Add at the end of Appendix C to Part 5, the following new paragraph "49":

Appendix C to Part 5—DHS Systems of Records Exempt From the Privacy Act

* * * * *

49. The DHS/USCIS—009 Compliance Tracking and Management System of Records consists of electronic and paper files that will be used by DHS and its components. This system of records will be used to perform a range of information management and analytic functions involving minimizing misuse, abuse, discrimination, breach of privacy, and fraudulent use of SAVE and E-Verify. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(2). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interest of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures

pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010–20856 Filed 8–20–10; 8:45 am]

BILLING CODE 9111–97–P

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 34

[Docket ID OCC–2010–0007]

RIN 1557–AD23

FEDERAL RESERVE SYSTEM

12 CFR Parts 208 and 211

[Docket No. R–1357]

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR Part 365

RIN 3064–AD43

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

12 CFR Part 563

[Docket No. 2010—0021]

RIN 1550–AC33

FARM CREDIT ADMINISTRATION

12 CFR Part 610

RIN 3052–AC52

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Parts 741 and 761

RIN 3133–AD59

Registration of Mortgage Loan Originators

Correction

In rule document 2010–18148 beginning on page 44656 in the issue of Wednesday, July 28, 2010, make the following corrections:

On pages 44656 through 44684, in Separate Part IV, footnotes 1 through 67 were not correctly numbered. The entire preamble is being reprinted to include the correctly numbered footnotes.

AGENCY: Office of the Comptroller of the Currency, Treasury (OCC); Board of Governors of the Federal Reserve System (Board); Federal Deposit Insurance Corporation (FDIC); Office of Thrift Supervision, Treasury (OTS); Farm Credit Administration (FCA); and National Credit Union Administration (NCUA).

ACTION: Final rule.

SUMMARY: The OCC, Board, FDIC, OTS, FCA, and NCUA (collectively, the Agencies) are adopting final rules to implement the Secure and Fair Enforcement for Mortgage Licensing Act (the S.A.F.E. Act). The S.A.F.E. Act requires an employee of a bank, savings association, credit union or Farm Credit System (FCS) institution and certain of their subsidiaries that are regulated by a Federal banking agency or the FCA (collectively, Agency-regulated institutions) who acts as a residential mortgage loan originator to register with the Nationwide Mortgage Licensing System and Registry, obtain a unique identifier, and maintain this registration. The final rule further provides that Agency-regulated institutions must: require their employees who act as residential mortgage loan originators to comply with the S.A.F.E. Act's requirements to register and obtain a unique identifier, and adopt and follow written policies and procedures designed to assure compliance with these requirements.

DATES: This final rule is effective on October 1, 2010. Compliance with § __.103 (registration requirement) of the final rule is required by the end of the 180-day period for initial registrations beginning on the date the Agencies provide in a public notice that the Registry is accepting initial registrations.

FOR FURTHER INFORMATION CONTACT:

OCC: Michele Meyer, Assistant Director, Heidi Thomas, Special Counsel, or Patrick T. Tierney, Senior Attorney, Legislative and Regulatory Activities, (202) 874–5090, and Nan Goulet, Senior Advisor, Large Bank Supervision, (202) 874–5224, Office of the Comptroller of the Currency, 250 E Street SW., Washington, DC 20219.

Board: Anne Zorc, Counsel, Legal Division, (202) 452–3876, Virginia Gibbs, Senior Supervisory Analyst, (202) 452–2521, and Stanley Rediger, Supervisory Financial Analyst, (202) 452–2629, Division of Banking Supervision and Regulation, Board of Governors of the Federal Reserve System, 20th and C Streets, NW., Washington, DC 20551.

FDIC: Thomas F. Lyons, Examination Specialist, (202) 898–6850, Victoria Pawelski, Senior Policy Analyst, (202) 898–3571, or John P. Kotsiras, Financial Analyst, (202) 898–6620, Division of Supervision and Consumer Protection; or Richard Foley, Counsel, (202) 898–3784, or Kimberly A. Stock, Counsel, (202) 898–3815, Legal Division, Federal Deposit Insurance Corporation, 550 17th Street, NW., Washington, DC 20429.

OTS: Charlotte M. Bahin, Special Counsel (Special Projects), (202) 906–6452, Vicki Hawkins-Jones, Special Counsel, Regulations and Legislation Division, (202) 906–7034, Debbie Merkle, Project Manager, Credit Risk, (202) 906–5688, and Rhonda Daniels, Senior Compliance Program Analyst, Consumer Regulations, (202) 906–7158, Office of Thrift Supervision, 1700 G Street, NW., Washington, DC 20552.

FCA: Gary K. Van Meter, Deputy Director, Office of Regulatory Policy, (703) 883–4414, TTY (703) 883–4434, or Richard A. Katz, Senior Counsel, or Jennifer Cohn, Senior Counsel, Office of General Counsel, (703) 883–4020, TTY (703) 883–4020, Farm Credit Administration, 1501 Farm Credit Drive, McLean, VA 22102–5090.

NCUA: Regina Metz, Staff Attorney, Office of General Counsel, 703–518–6561, or Lisa Dolin, Program Officer, Division of Supervision, Office of Examination and Insurance, 703–518–6360, National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314–3428.

SUPPLEMENTARY INFORMATION:

I. Background

A. Statutory Requirements

The S.A.F.E. Act,[1] enacted on July 30, 2008, mandates a nationwide licensing and registration system for mortgage loan originators. Specifically, the Act requires all States to provide for a licensing and registration regime for mortgage loan originators who are not employed by Agency-regulated institutions within one year of enactment (or two years for States whose legislatures meet biennially). In addition, the S.A.F.E. Act requires the OCC, Board, FDIC, OTS and NCUA,[2] through the Federal Financial Institutions Examination Council (FFIEC), and the FCA to develop and

[1] The S.A.F.E. Act was enacted as part of the Housing and Economic Recovery Act of 2008, Public Law 110–289, Division A, Title V, sections 1501–1517, 122 Stat. 2654, 2810–2824 (July 30, 2008), *codified at* 12 U.S.C. 5101–5116. Citations in this Supplementary Information section are to the "S.A.F.E. Act" by section number in the public law.

[2] The OCC, Board, FDIC, OTS, and NCUA are referred to both in the S.A.F.E. Act and in this rulemaking as the "Federal banking agencies."