



# Self-Assessment Guide

For SAVE Program Web and Web Services-based Users

*July 2012*



U.S. Citizenship  
and Immigration  
Services

**M-1063**

---

---

# Table of Contents

<b>I. INTRODUCTION</b> .....	<b>1</b>
PURPOSE OF THIS DOCUMENT.....	1
BACKGROUND.....	1
COMPLIANCE ELEMENTS .....	1
SELF-ASSESSMENT GUIDE BENEFITS .....	1
<b>II. HOW TO USE THE SELF-ASSESSMENT GUIDE</b> .....	<b>2</b>
<b>III. SELF-ASSESSMENT CHECKLIST STANDARDS</b> .....	<b>3</b>
PART 1: TRAINING.....	3
PART 2: VERIFICATION PROCEDURES.....	5
PART 3: SECURITY AND PRIVACY.....	7
PART 4: APPLICANT ASSISTANCE .....	11
PART 5: NOTIFICATIONS TO SAVE .....	13
PART 6: LEGAL RESTRICTIONS AND COMPLIANCE.....	15
<b>IV. REFERENCED AND SUPPORTING DOCUMENTATION</b> .....	<b>16</b>
<b>V. GLOSSARY</b> .....	<b>17</b>
COMMONLY USED ACRONYMS AND TERMS.....	17

---

# I. INTRODUCTION

## PURPOSE OF THIS DOCUMENT

The Systematic Alien Verification for Entitlements (SAVE) Program developed this SAVE Self-Assessment Guide as a tool for agencies to perform internal monitoring and compliance assessments to support proper use of SAVE and improve the overall integrity of their SAVE verifications.

The Memorandum of Agreement (MOA) between your agency and the Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS), SAVE Program, establishes the terms and conditions for your agency's use of SAVE. The Verification Division Monitoring and Compliance (M&C) Branch monitors the use of SAVE to ensure its proper use. Agencies using SAVE are encouraged to establish their own internal monitoring and compliance program.

## BACKGROUND

Agencies using SAVE are responsible for ensuring that all SAVE users follow all SAVE requirements. The MOA specifies that your agency must ensure that everyone performing verification procedures is complying with all requirements in the SAVE MOA, SAVE Program Guide (Program Guide), and web-based tutorial and updates to these requirements. (See Section II B.(1)(f) of the MOA).

## COMPLIANCE ELEMENTS

The SAVE Program has identified general requirements that agencies should follow when using SAVE. Although the general requirements for the use of SAVE are established by an agency's MOA, the questions and standards in this guide are framed to help the agency identify and address noncompliant activities. For the most part, noncompliant activities are general misuse of SAVE, but in some instances could be more serious in nature.

Because there are instances when an agency's particular needs regarding the use of SAVE require a revision of certain provisions of the agency's MOA, an individual agency's MOA may not follow the standard MOA format. Therefore, you must look at your agency's MOA to determine whether any aspects of this guide may have to be altered to suit your agency's circumstances.

## SELF-ASSESSMENT GUIDE BENEFITS

Implementation of a voluntary self-assessment program helps agencies to:

- Detect misuse and noncompliant activities concerning SAVE
- Resolve noncompliant activities quickly and effectively
- Promote proper use and prevent noncompliance
- Detect and resolve redundant administrative processes
- Improve compliance with SAVE policies and procedures
- Increase assurance that only eligible applicants receive benefits

---

## **II. HOW TO USE THE SELF-ASSESSMENT GUIDE**

This Self-Assessment Guide has six parts; each part addresses a topical area suggested for your internal monitoring and compliance program. Each part includes a checklist to guide your review of the activities related to the topical area. The checklists are for your agency's internal use; you are not required to send the compliance checklist to SAVE.

- Part 1: Training
- Part 2: Verification Procedures
- Part 3: Security and Privacy
- Part 4: Applicant Assistance
- Part 5: Notifications to SAVE
- Part 6: Legal Restrictions and Compliance

### III. SELF-ASSESSMENT CHECKLIST STANDARDS

#### PART 1: TRAINING

All SAVE users must be properly trained before using SAVE. This will help ensure that benefit applicants are not inappropriately denied or awarded benefits. The MOA and the Program Guide require everyone performing verification procedures to complete required SAVE training before using SAVE. (See Section IV.B.(1)(d) of the MOA and Section 4 of the Program Guide). This training includes:

- 1) reading the SAVE Program Guide,
- 2) taking the latest version of SAVE Training tutorial(s) and
- 3) Refreshing knowledge of these requirements each time they are updated.

Also refer to the Program Guide at Section 5.1.

**Note:** The MOA incorporates by reference any requirements in the Program Guide and web-based tutorials. To ensure compliance, your agency must monitor SAVE notifications to be aware when SAVE updates requirements and training tutorials and ensure that SAVE users are aware of these updates. SAVE may make these notices in the form of ticker messages on the SAVE access method, by email, letter, or via the SAVE website ([www.uscis.gov/save](http://www.uscis.gov/save)).

#	Question	Response Selection	Response Notes
1.1	Has everyone performing verification procedures read the latest version of the SAVE Program Guide, before using SAVE?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
1.2	Has everyone performing verification procedures taken the latest version of Web tutorial(s) before using SAVE?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
1.3	Is your agency monitoring the SAVE notices and ensuring that everyone using SAVE is aware of all updates?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
1.4	Does everyone performing verification procedures have a working knowledge of requirements contained in the latest version of the SAVE Program Guide?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
1.5	Does everyone performing verification procedures have a working knowledge of requirements contained in the tutorial(s), as updated?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
1.6	Does everyone performing verification procedures have a working knowledge of requirements contained in the MOA, as updated?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	

#	Question	Response Selection	Response Notes
1.7	Is your agency ensuring that everyone using SAVE is complying with all requirements in questions 1.4, 1.5 and 1.6, as updated?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	

---

## PART 2: VERIFICATION PROCEDURES

SAVE verification process requirements must be followed to ensure the integrity of the verification process. If SAVE verification process requirements are not followed, applicants could be inappropriately denied or awarded benefits.

The MOA requires that all SAVE users establish the identity of the benefit applicants and require the applicants to present immigration or naturalization documentation that contains the applicants' information (e.g., alien registration number, passport number or I-94 number) before beginning a request for verification. (See Section IV.B.(1)(a) of the MOA and Section 3.1 of the Program Guide).

Additionally, the MOA requires users to physically examine the documents presented by the benefit applicant and determine whether the document(s) reasonably appear(s) to be genuine and relate to the individual. (See Section IV.B.(1)(b) of the MOA and Section 3.5.2 of the Program Guide).

SAVE has a three step process. Depending on the circumstances, you may need to use one, two, or all three steps to make certain that all available records have been searched to verify an applicant. These steps are

1. Electronic initial verification -
2. Electronic second step verification -
3. Manual third step verification.

Unless these additional verification steps are followed as required by SAVE, the verification process may be incomplete and the integrity of the process compromised. Accordingly, the MOA and the Program Guide require users to perform all required additional verification procedures that the benefit applicant requests after initiating electronic verification. This additional verification includes second step electronic verifications and third step submission of copies of the benefit applicants' immigration documents to SAVE. (See Section IV.B.(1)(h) of the MOA and Section 3.3 and 5.1 of the Program Guide).

Sometimes it is necessary to go straight to the third step, manual verification. The Program Guide requires users to skip automated initial verification and second step verification and instead submit a Form G-845 when a benefit applicant presents:

- A document that appears to be counterfeit or altered, which can be indicated by a photo substitution or discolored ink
- An unfamiliar DHS document
- A document that indicates immigration status, but does not contain an A-Number
- A foreign passport and/or Form I-94 with an "Admission for Permanent Residence" endorsement more than one year old

(See Section 3.5.2 of the Program Guide)

Occasionally a SAVE response does not match the information on the benefit applicant's immigration document. The Program Guide requires users to initiate additional verification without being prompted to by SAVE when there is a material discrepancy between information on a benefit applicant's immigration document and the SAVE response. (See Section 3.3 of the Program Guide).

	Question	Response Selection	Response Notes
2.1	Is the identity of the benefit applicant established before running a SAVE query on the applicant?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
2.2	Does everyone require the benefit applicant to present his/her immigration or naturalization document that contains the information (e.g., alien registration number, passport number or I-94 number, etc.) required by the SAVE Program?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
2.3	Does everyone physically examine the document presented by the benefit applicant to determine whether the document reasonably appears to be genuine and relate to the benefit applicant?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
2.4	After beginning electronic verification requests, are all users performing all additional verification procedures the SAVE Program requires and/or the applicants request, including second step electronic verifications and third step submission of copies of the benefit applicants' immigration documents to SAVE?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
2.5	Are all users skipping automated initial verification and second step verification and submitting a Form G-845 when a benefit applicant presents:  a) a document that appears to be counterfeit or altered, b) an unfamiliar DHS document, c) a document that indicates immigration status, but does not contain an A or I-94 Number, d) a foreign passport and/or Form I-94 with an "Admission for Permanent Residence" endorsement more than one year old?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
2.6	Is everyone initiating additional verification when there is a material discrepancy between information on the benefit applicant's immigration documents and the SAVE response?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	



---

## PART 3: SECURITY AND PRIVACY

This section addresses actions your agency must take to ensure that information provided by SAVE is properly protected from unauthorized disclosure.

To prevent access to SAVE by unauthorized individuals, the MOA requires that SAVE users are provided with and maintain User IDs only while they have a need to perform verification procedures. (See Section IV.B.(1)(e)). Accordingly, an individual's User ID should be terminated immediately when they no longer need to perform verifications. Also refer to the Guide at Section 5.2.

The MOA directs your agency to follow the requirements of the Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) guidance as applicable to electronic storage, transport of records between agencies, and the internal processing of records received by the agency under the terms of the MOA. (See Section IV.B.(1)(j)).

FISMA generally speaks to the legal obligations of the federal government. As reflected in the MOA, state and local governments eligible for participation in SAVE must agree to ensure the integrity of DHS data through compliance with federal privacy laws.

To be FISMA compliant, state and local agencies should refer to the Department of Commerce, National Institute of Standards and Technology (NIST) guidelines. Your agency is responsible for implementing the NIST guidance in a manner best suited to its available resources and needs. According to the NIST guidance, agencies should:

- Conduct periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems that support the operations and assets of the organization.
- Develop policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the lifecycle of each organizational information system.
- Have subordinate plans for providing adequate information security for networks, facilities, information systems or groups of information systems, as appropriate.
- Conduct security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks.
- Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, practices and security controls to be performed with a frequency depending on risk, but no less than annually.
- Develop a process for planning, implementing, evaluating and documenting remedial actions to address any deficiencies in the information security policies, procedures and practices of the organization.
- Develop procedures for detecting, reporting and responding to security incidents.
- Develop plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization.

The MOA also requires your agency to follow the Privacy Act and other applicable laws, regulations and policies, including but not limited to all OMB and DHS privacy guidance, in conducting verifications and safeguarding, maintaining and disclosing any data provided

---

under the MOA. (See Section IV.B.(1)(l) of the MOA and 5 U.S.C. Section 552a of the Privacy Act).

The Privacy Act speaks to the legal obligations of the federal government. However, state and local governments eligible for participation in SAVE must agree to ensure the integrity of DHS data through compliance with federal privacy laws.

The Privacy Act governs the means by which the U.S. government collects, maintains, uses and disseminates the personally identifiable information (PII) of U.S. citizens and lawful permanent residents (LPRs). However, under DHS policy, to the extent practicable, privacy protections afforded to U.S. citizens and LPRs must also be afforded to visitors and aliens when there is a mixed system containing information on U.S. persons and visitors and aliens.

Refer to the Fact Sheet, “Information for SAVE Users: Your Responsibilities for Handling and Protecting Personal Information,” and Part 5: Notifications to SAVE below for additional information on PII. Compliance with the FISMA elements described above and other requirements of the MOA will largely ensure that the privacy of an individual’s PII is safeguarded. Any documents containing PII obtained as part of or the result of a SAVE verification must receive the same level of protection as electronic SAVE information. Please note that under Department of Homeland Security Management Directive, MD 11042.1, “Safeguarding Sensitive but Unclassified (For Official Use Only) Information,” (2005) your agency should mark documents containing PII with privacy language such as “For Official Use Only” to identify the need to protect the information from inappropriate disclosure. Also refer to the Fact Sheet, “Information for SAVE Users: Your Responsibilities for Handling and Protecting Personal Information,” for additional information.

### **Safeguarding SAVE information**

The MOA requires your agency to safeguard SAVE information and access methods to ensure that it is not used for any other purpose than described in the MOA. It also requires your agency to protect the information’s confidentiality, ensuring that it is not disclosed to any unauthorized person(s) without the prior written consent of DHS-USCIS. (See Section IV.B.(1)(k)).

The MOA further requires that your agency ensures that information provided by DHS-USCIS is used solely for determining the eligibility of persons applying for the benefit(s) specified in the MOA. (See Section IV.B.(1)(i)).

Additionally, the MOA specifies that any person who obtains SAVE information covered by the Privacy Act under false pretenses or uses it for any purpose other than as provided for in the MOA may be subject to criminal penalties. (See section VI.(C)(2)).

Under the Privacy Act your agency must:

- Notify individuals applying for benefits that the personal information that your agency is collecting will be used to verify their immigration status through SAVE.
- Advise individuals applying for benefits that they do not have to provide the information.
- Advise individuals applying for benefits of the consequences of not providing the information.

Also refer to the Fact Sheet, “Information for SAVE Users: Your Responsibilities for Handling and Protecting Personal Information,” for additional information.

**Please Note:** Benefit applicants seeking information about themselves should be directed to the Freedom of Information and Privacy Act page of [www.uscis.gov](http://www.uscis.gov) for directions on submitting a Privacy Act request to DHS-USCIS. For additional information regarding prohibitions on the use of SAVE, please also reference the Legal Restrictions and Compliance Section of this Checklist and the Program Guide at Section 5.2.

#	Question	Response Selection	Response Notes
3.1	Are User IDs only provided to authorized users with a specific need-to-know?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
3.2	Are User IDs terminated when SAVE access is no longer required?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
3.3	Are passwords protected by each authorized user and not shared with anyone else?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
3.4	Is your agency complying with the requirements of FISMA and OMB guidance as applicable to electronic storage, transport of records between agencies and the internal processing of records received by the agency under the terms of the MOA?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
3.5	Is your agency protecting the confidentiality of PII (e.g., names, date of birth, Social Security numbers, alien or I-94 numbers, passport numbers, phone numbers, employment history, and email and physical addresses)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
3.6	Is your agency ensuring that it is not disclosing information provided by SAVE to any unauthorized person(s) without the prior written consent of DHS-USCIS?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
3.7	Is your agency safeguarding SAVE access methods and information provided by SAVE to ensure that it is not used for any other purpose than described in the MOA?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	

#	Question	Response Selection	Response Notes
3.8	Is your agency complying with the Privacy Act and other applicable laws, regulations and policies in safeguarding, maintaining and disclosing any data provided or received under the MOA?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
3.9	Is your agency marking documents with PII with language such as "For Official Use Only?"	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
3.10	Is your agency complying with the requirement to notify benefit applicants that their PII is being collected to run a SAVE query?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
3.11	Is your agency complying with the requirement to notify benefit applicants that they may refuse to provide their PII and of the consequences of refusal to provide the information?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
3.12	Are benefit applicants seeking information about themselves directed to the Freedom of Information and Privacy Act page of <a href="http://www.uscis.gov">www.uscis.gov</a> for directions on submitting a Privacy Act request to DHS-USCIS?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	

---

## **PART 4: APPLICANT ASSISTANCE**

This section addresses actions that your agency must take to ensure that benefit applicants are given adequate assistance and provided a fair opportunity to present the information necessary for them to be verified with SAVE.

When a benefit applicant presents an expired document or is unable to present any immigration documentation supporting his or her immigration status, your agency must ensure that SAVE users refer the applicant to the local USCIS Office to obtain documentation of his/her immigration status as required by the Program Guide at 3.5.1. There may be instances where this is not appropriate, i.e., when Temporary Protected Status or Deferred Enforced Departure is extended for particular countries. Please monitor all updates to SAVE requirements to ensure that a benefit applicant is not inappropriately referred to USCIS.

When an applicant is denied a benefit solely or in part on the basis of a SAVE response, your agency must ensure that the applicant is provided with adequate written notice of the denial and the instructions on how to contact DHS-USCIS so that the applicant may correct his/her records promptly, if necessary. (See Section IV.B.(1)(n) of the MOA). The fact sheet attached to your MOA, "Information for Applicants: Verification of Immigration Status and How to Correct Your Record with USCIS," (which is subject to revision and reposting on the SAVE website and Online Resources) should be given to the applicants to inform them how to contact DHS-USCIS. (See also the Program Guide at Section 5).

Additionally, when an applicant is denied a benefit solely or in part on the basis of the SAVE response, the applicant must be given the opportunity to use the agency's existing process to appeal the denial of the benefit and to contact DHS-USCIS to correct his/her records before a final decision. (See Section IV.B.(1)(o) of the MOA and the Program Guide at Section 5.1, 5.1.1 and 5.4).

#	Question	Response Selection	Response Notes
4.1	When a benefit applicant presents an expired document or is unable to present any immigration document supporting his/ her immigration status, is the applicant referred to the local USCIS Office to obtain documentation of his/her immigration status?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
4.2	Are all applicants who are denied benefits based solely or in part on the SAVE response provided with adequate written notice of the denial and the information necessary to contact DHS-USCIS so that the individuals may correct their records promptly?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
4.3	Are all applicants who are denied benefits based solely or in part on the SAVE response provided with the opportunity to use the agency's existing process to appeal the denial and to contact DHS-USCIS to correct their records before a final decision?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
4.4	Are all applicants who are denied benefits based solely or in part on the SAVE response given a copy of "Information for Applicants: Verification of Immigration Status and How to Correct Your Record with USCIS?"	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	

---

## **PART 5: NOTIFICATIONS TO SAVE**

This section concerns actions your agency must take to ensure that SAVE and SAVE Monitoring and Compliance (M&C) are notified of matters involving contact information, changes to agency benefits and breaches involving SAVE provided PII.

SAVE needs to be able to readily contact your agency regarding a variety of matters. Accordingly, the MOA requires that your agency notify SAVE and SAVE M&C when there is a change in any of the following: name and telephone number of the agency authorized representative, current email, U.S. postal service address and physical address. (See Section IV.B.(2)(a) of the MOA).

Because anyone using SAVE may have a need to contact SAVE or SAVE M&C based on SAVE requirements or the individual user's needs, the MOA requires users performing verification procedures to have contact information for the SAVE Program and SAVE M&C. (See Section IV.B.(1)(g) of the MOA). The MOA lists points of contact for SAVE and SAVE M&C. (See at Section V of the MOA). This information, and any updates through the methods identified above, must be provided to all SAVE users.

As indicated in the Security and Privacy section above and in the Legal Restrictions and Compliance section below, SAVE can only be used for the purpose described in the MOA. Typically, the approved uses are specified in the description of the benefit(s). Accordingly, the MOA requires your agency to notify SAVE and SAVE M&C of any changes to the agency benefit(s) identified in the MOA. (See Section IV.B.(2)(a) of the MOA). Before your agency can use SAVE for any purpose not described in the MOA, SAVE must review and approve your agency's legal authorities to verify status and administer the benefit(s) and a new MOA must be completed. Also refer to the Program Guide at Section 5.2.

To ensure that individuals are not harmed by a breach of security or privacy requirements, the MOA requires your agency to notify SAVE and SAVE M&C immediately whenever there is reason to believe a violation of this MOA has occurred or if there is reason to believe an information breach has occurred as a result of agency action or inaction under OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." (See Section IV.B.(2)(c) of the MOA).

OMB Memorandum M-07-16 speaks to the legal obligations of the federal government, however, state and local government agencies eligible for participation in SAVE must agree to ensure the integrity of DHS data through compliance with federal privacy laws. For purposes of their use of SAVE that means that in addition to the elements identified above for compliance with FISMA, state and local government agencies must have a policy and plan in place to ensure that SAVE and SAVE M&C are immediately notified when a breach of PII occurs and that benefit applicants negatively affected by the breach of their PII are notified so that any harm can be mitigated.

OMB Memorandum M-07-16 defines PII as, "information which can be used to distinguish or trace an individual's identity, such as name, Social Security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." (See also the Program Guide at Section 5.2).

#	Question	Response Selection	Response Notes
5.1	Is the agency providing the SAVE Program and SAVE M&C with the current email, U.S. postal service address, physical address, name and telephone number of the agency's authorized representative?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
5.2	Does everyone performing verification procedures have contact information for the SAVE Program and SAVE M&C, as updated?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
5.3	Is your agency notifying SAVE and SAVE M&C of changes in the benefit(s) identified in the MOA before using SAVE to run verifications based on these changes?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
5.4	Is your agency notifying the SAVE Program and SAVE M&C immediately when there is reason to believe a violation of this MOA has occurred?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
5.5	Is your agency notifying the SAVE Program and SAVE M&C when there is reason to believe a breach of PII provided by SAVE has occurred?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
5.6	Is your agency notifying the benefit applicants when a breach of their PII provided by SAVE has occurred?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	



## PART 6: LEGAL RESTRICTIONS AND COMPLIANCE

This section concerns certain legal prohibitions that must be observed by your agency and the obligation to ensure that written recommendations to correct noncompliance are implemented.

As indicated in the Security and Privacy section above, SAVE can only be used for the purposes described in your MOA. Additionally, the MOA identifies specific prohibitions on the use of SAVE. The MOA requires your agency to follow federal laws prohibiting discrimination against benefit applicants and discriminatory use of SAVE based upon the national origin, color, race, gender, religion or disability of the applicant. (See Section IV.B.(1)(m) of the MOA). Inconsistent use of SAVE can be an indicator of discrimination if it disproportionately affects applicants in the identified categories. Accordingly, your agency must consistently follow all SAVE Program requirements and monitor any inconsistencies. (See the Program Guide at 3.5.2 and 5.1.2).

Under current law, verification with DHS-USCIS for employment eligibility must be done through E-Verify. Accordingly, the MOA states that your agency must not use SAVE, or assist any person or entity, to follow the employment eligibility verification requirements of Section 274A of the Immigration and Nationality Act, 8 U.S.C. Section 1324a. For information on E-Verify visit [www.uscis.gov/everify](http://www.uscis.gov/everify).

To have an effective monitoring and compliance program, your agency must correct any identified noncompliant activities. The MOA requires your agency to promptly correct every written finding of noncompliance with the terms, conditions and safeguards of the MOA. (See Section IV.B.(2)(i) of the MOA). Accordingly, your agency must have a process to correct noncompliance issues as they are identified without any undue delay.

#	Question	Response Selection	Response Notes
6.1	Is your agency ensuring that everyone is complying with all SAVE requirements so that SAVE is not used in a manner that discriminates based upon the national origin, color, race, gender, religion or disability of the applicant?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
6.2	Is the agency ensuring that SAVE is not being used to verify employment eligibility for the purpose of hiring?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	
6.3	Is the agency promptly correcting noncompliant behavior regarding its use of SAVE?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Other	

---

## IV. REFERENCED AND SUPPORTING DOCUMENTATION

The following materials are referenced as part of the Self-Assessment Checklists:

- Memorandum of Agreement with SAVE
- SAVE Program Guide
- Office of Management and Budget (OMB) Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information"
- Form G-845 "Document Verification Request" and Form G-845 Supplement "Document Verification Request Supplement"
- SAVE Training Tutorial(s)
- Fact Sheet, "Information for SAVE Users: Your Responsibilities for Handling and Protecting Personal Information"
- Department of Homeland Security Management Directive, MD 11042.1, "Safeguarding Sensitive But Unclassified (For Official Use Only) Information" (2005)

## V. GLOSSARY

### COMMONLY USED ACRONYMS AND TERMS

The following table contains the acronyms commonly used throughout this document.

Acronym	Definition
DHS	Department of Homeland Security
Guide	SAVE Program Guide
M&C	Monitoring and Compliance Branch
MOA	Memorandum of Agreement
USCIS	U.S. Citizenship and Immigration Services

In addition, this document contains several terms that have specific meaning for the compliance process and/or business context of the USCIS Verification Division.

**Web Access** – A web-based access method that allows agencies to submit verification queries through a Web browser such as Internet Explorer or Netscape.

**Web Services Access** – An access method that allows agencies to build their own systems to integrate with the SAVE Program. Through Web Services, agencies are able to extract information from their existing system and transmit data to the SAVE Program to perform verifications. Web Services users design their own screens and do not see the standard screens of the Web-based Access method.

**Agency** – A federal, state or local government entity that has a signed MOA with DHS allowing it to participate in the SAVE Program as a customer of the Verification Division.

**Users** – Individuals authorized by a participating Agency to access the SAVE Program for the uses specified in the Agency's MOA with DHS.

**Monitoring and Compliance (M&C)** – The branch of the Verification Division of U.S. Citizenship and Immigration Services responsible for the administration of the monitoring and compliance assistance processes as part of its comprehensive business process.