



Company ID Number: \_\_\_\_\_

**THE E-VERIFY  
MEMORANDUM OF UNDERSTANDING  
FOR WEB SERVICES EMPLOYERS**

**ARTICLE I  
PURPOSE AND AUTHORITY**

The parties to this Agreement are the Department of Homeland Security (DHS) and \_\_\_\_\_ (Web Services Employer). The purpose of this agreement is to set forth terms and conditions which the Web Services Employer will follow while participating in E-Verify.

A Web Services Employer is an Employer who verifies employment authorization for its newly hired employees using a Web Services interface.

E-Verify is a program that electronically confirms a newly hired employee's authorization to work in the United States after completion of the Form I-9, Employment Eligibility Verification (Form I-9). This MOU explains certain features of the E-Verify program and describes specific responsibilities of the Web Services Employer, DHS, and the Social Security Administration (SSA).

For purposes of this MOU, the "E-Verify browser" refers to the website that provides direct access to the E-Verify system: <https://e-verify.uscis.gov/emp/>. You may access E-Verify directly free of charge via the E-Verify browser.

Authority for the E-Verify program is found in Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Pub. L. 104-208, 110 Stat. 3009, as amended (8 U.S.C. § 1324a note). The Federal Acquisition Regulation (FAR) Subpart 22.18, "Employment Eligibility Verification" and Executive Order 12989, as amended, provide authority for Federal contractors and subcontractors (Federal contractor) to use E-Verify to verify the employment eligibility of certain employees working on Federal contracts.

Before accessing E-Verify using Web Services access, the Web Services Employer must meet certain technical requirements. This will require the investment of significant amounts of resources and time. If the Web Services Employer is required to use E-Verify prior to completion and acceptance of its Web Services interface, then it must use the E-Verify browser until it is able to use its Web Services interface. The Web Services Employer must also maintain ongoing technical compatibility with E-Verify.

DHS accepts no liability relating to the Web Services Employer's development or maintenance of any Web Services access system.

## **ARTICLE II**

### **RESPONSIBILITIES**

#### **A. RESPONSIBILITIES OF THE WEB SERVICES EMPLOYER**

1. By enrolling in E-Verify and signing the applicable MOU, the Web Services Employer asserts that it is a legitimate company which intends to use E-Verify for legitimate purposes only and in accordance with the laws, regulations, and DHS policies and procedures relating to the use of E-Verify.
2. The Web Services Employer agrees to display the following notices supplied by DHS in a prominent place that is clearly visible to prospective employees and all employees who are to be verified through the system:
  - a. Notice of E-Verify Participation
  - b. Notice of Right to Work
3. The Web Services Employer agrees to provide to the SSA and DHS the names, titles, addresses, and telephone numbers of the Web Services Employer representatives to be contacted about E-Verify. The Web Services Employer also agrees to keep such information current by providing updated information to SSA and DHS whenever the representatives' contact information changes.
4. The Web Services Employer agrees to grant E-Verify access only to current employees who need E-Verify access. Web Services Employers must promptly terminate an employee's E-Verify access if the employer is separated from the company or no longer needs access to E-Verify.
5. The Web Services Employer agrees to become familiar with and comply with the most recent version of the E-Verify User Manual. The Web Services Employer will ensure that outdated manuals are promptly replaced with the new version of the E-Verify User Manual when it becomes available.
6. The Web Services Employer agrees that any person accessing E-Verify on its behalf is trained on the most recent E-Verify policy and procedures.
7. The Web Services Employer agrees that any of its representatives who will create E-Verify cases will complete the E-Verify Tutorial before creating any cases.
  - a. The Web Services Employer agrees that all of its representatives will take the refresher tutorials when prompted by E-Verify in order to continue using E-Verify. Failure to complete a refresher tutorial will prevent the Employer Representative from continued use of E-Verify.
8. The Web Services E-Verify Employer Agent agrees to obtain the necessary equipment to use E-Verify as required by the E-Verify rules and regulations as modified from time to time.
9. The Web Services E-Verify Employer Agent agrees to, consistent with applicable laws, regulations, and policies, commit sufficient personnel and resources to meet the requirements of this MOU.

10. The Web Services Employer agrees to comply with current Form I-9 procedures, with two exceptions:

- a. If an employee presents a "List B" identity document, the Web Services Employer agrees to only accept "List B" documents that contain a photo. (List B documents identified in 8 C.F.R. § 274a.2(b)(1)(B)) can be presented during the Form I-9 process to establish identity.) If an employee objects to the photo requirement for religious reasons, the Web Services Employer should contact E-Verify at 888-464-4218.
- b. If an employee presents a DHS Form I-551 (Permanent Resident Card), Form I-766 (Employment Authorization Document), or U.S. Passport or Passport Card to complete Form I-9, the Web Services Employer agrees to make a photocopy of the document and to retain the photocopy with the employee's Form I-9. The Web Services Employer will use the photocopy to verify the photo and to assist DHS with its review of photo mismatches that employees contest. DHS may in the future designate other documents that activate the photo screening tool.

Note: Subject only to the exceptions noted previously in this paragraph, employees still retain the right to present any List A, or List B and List C, document(s) to complete the Form I-9.

11. The Web Services Employer agrees to record the case verification number on the employee's Form I-9 or to print the screen containing the case verification number and attach it to the employee's Form I-9.

12. The Web Services Employer agrees that, although it participates in E-Verify, the Web Services Employer has a responsibility to complete, retain, and make available for inspection Forms I-9 that relate to its employees, or from other requirements of applicable regulations or laws, including the obligation to comply with the antidiscrimination requirements of section 274B of the INA with respect to Form I-9 procedures.

- a. The following modified requirements are the only exceptions to an Web Services Employer's obligation to not employ unauthorized workers and comply with the anti-discrimination provision of the INA: (1) List B identity documents must have photos, as described in paragraph 6 above; (2) When a Web Services Employer confirms the identity and employment eligibility of newly hired employee using E-Verify procedures, it establishes a rebuttable presumption that it has not violated section 274A(a)(1)(A) of the Immigration and Nationality Act (INA) with respect to the hiring of that employee; (3) If the Web Services Employer receives a final nonconfirmation for an employee, but continues to employ that person, the Web Services Employer must notify DHS and the Web Services Employer is subject to a civil money penalty between \$550 and \$1,100 for each failure to notify DHS of continued employment following a final nonconfirmation; (4) If the Web Services Employer continues to employ an employee after receiving a final nonconfirmation, then the Web Services Employer is subject to a rebuttable presumption that it has knowingly employed an unauthorized alien in violation of section 274A(a)(1) (A); and (5) no E-Verify participant is civilly or criminally liable under any law for any action taken in good faith based on information provided through the E-Verify.
- b. DHS reserves the right to conduct Form I-9 compliance inspections, as well as any other enforcement or compliance activity authorized by law, including site visits, to ensure proper use of E-Verify.

13. The Web Services Employer is strictly prohibited from creating an E-Verify case before the employee has been hired, meaning that a firm offer of employment was extended and accepted and Form I-9 was completed. The Employer agrees to create an E-Verify case for new

employees within three Employer business days after each employee has been hired (after both Sections 1 and 2 of Form I-9 have been completed), and to complete as many steps of the E-Verify process as are necessary according to the E-Verify User Manual. If E-Verify is temporarily unavailable, the three-day time period will be extended until it is again operational in order to accommodate the Employer's attempting, in good faith, to make inquiries during the period of unavailability. If, however, the Web Services interface is unavailable due to no fault of E-Verify, then the three day time period is not extended. In such a case, the Web Services Employer must use the E-Verify browser during the outage.

14. The Web Services Employer agrees not to use E-Verify for pre-employment screening of job applicants, in support of any unlawful employment practice, or for any other use that this MOU or the E-Verify User Manual does not authorize.

15. The Web Services Employer must use E-Verify for all new employees. The Web Services Employer will not verify selectively and will not verify employees hired before the effective date of this MOU. Employers who are Federal contractors may qualify for exceptions to this requirement as described in Article II.B of this MOU.

16. The Web Services Employer agrees to follow appropriate procedures (see Article III below) regarding tentative nonconfirmations. The Web Services Employer must promptly notify employees in private of the finding and provide them with the notice and letter containing information specific to the employee's E-Verify case. The Web Services Employer agrees to provide both the English and the translated notice and letter for employees with limited English proficiency to employees. The Web Services Employer agrees to provide written referral instructions to employees and instruct affected employees to bring the English copy of the letter to the SSA. The Web Services Employer must allow employees to contest the finding, and not take adverse action against employees if they choose to contest the finding, while their case is still pending. Further, when employees contest a tentative nonconfirmation based upon a photo mismatch, the Employer must take additional steps (see Article III.B below) to contact DHS with information necessary to resolve the challenge.

17. The Web Services Employer agrees not to take any adverse action against an employee based upon the employee's perceived employment eligibility status while SSA or DHS is processing the verification request unless the Employer obtains knowledge (as defined in 8 C.F.R. § 274a.1(l)) that the employee is not work authorized. The Web Services Employer understands that an initial inability of the SSA or DHS automated verification system to verify work authorization, a tentative nonconfirmation, a case in continuance (indicating the need for additional time for the government to resolve a case), or the finding of a photo mismatch, does not establish, and should not be interpreted as, evidence that the employee is not work authorized. In any of such cases, the employee must be provided a full and fair opportunity to contest the finding, and if he or she does so, the employee may not be terminated or suffer any adverse employment consequences based upon the employee's perceived employment eligibility status (including denying, reducing, or extending work hours, delaying or preventing training, requiring an employee to work in poorer conditions, withholding pay, refusing to assign the employee to a Federal contract or other assignment, or otherwise assuming that he or she is unauthorized to work) until and unless secondary verification by SSA or DHS has been completed and a final nonconfirmation has been issued. If the employee does not choose to contest a tentative nonconfirmation or a photo mismatch or if a secondary verification is completed and a final nonconfirmation is issued, then the Web Services Employer can find the employee is not work authorized and terminate the employee's employment. Employers or employees with questions about a final nonconfirmation may call E-Verify at 1-888-464-4218 (customer service) or 1-888-897-7781 (worker hotline).

18. The Web Services Employer agrees to comply with Title VII of the Civil Rights Act of 1964 and section 274B of the INA as applicable by not discriminating unlawfully against any individual in hiring, firing, employment eligibility verification, or recruitment or referral practices because of his or her national origin or citizenship status, or by committing discriminatory documentary practices. The Web Services Employer understands that such illegal practices can include selective verification or use of E-Verify except as provided in part D below, or discharging or refusing to hire employees because they appear or sound “foreign” or have received tentative nonconfirmations. The Web Services Employer further understands that any violation of the immigration-related unfair employment practices provisions in section 274B of the INA could subject the Web Services Employer to civil penalties, back pay awards, and other sanctions, and violations of Title VII could subject the Web Services Employer to back pay awards, compensatory and punitive damages. Violations of either section 274B of the INA or Title VII may also lead to the termination of its participation in E-Verify. If the Web Services Employer has any questions relating to the anti-discrimination provision, it should contact OSC at 1-800-255-8155 or 1-800-237-2515 (TDD).

19. The Web Services Employer agrees that it will use the information it receives from E-Verify only to confirm the employment eligibility of employees as authorized by this MOU. The Web Services Employer agrees that it will safeguard this information, and means of access to it (such as PINS and passwords), to ensure that it is not used for any other purpose and as necessary to protect its confidentiality, including ensuring that it is not disseminated to any person other than employees of the Web Services Employer who are authorized to perform the Web Services Employer's responsibilities under this MOU, except for such dissemination as may be authorized in advance by SSA or DHS for legitimate purposes.

20. The Web Services Employer agrees to notify DHS immediately in the event of a breach of personal information. Breaches are defined as loss of control or unauthorized access to E-Verify personal data. All suspected or confirmed breaches should be reported by calling 1-888-464-4218 or via email at [E-Verify@dhs.gov](mailto:E-Verify@dhs.gov). Please use “Privacy Incident – Password” in the subject line of your email when sending a breach report to E-Verify.

21. The Web Services Employer acknowledges that the information it receives from SSA is governed by the Privacy Act (5 U.S.C. § 552a(i)(1) and (3)) and the Social Security Act (42 U.S.C. 1306(a)). Any person who obtains this information under false pretenses or uses it for any purpose other than as provided for in this MOU may be subject to criminal penalties.

22. The Web Services Employer agrees to cooperate with DHS and SSA in their compliance monitoring and evaluation of E-Verify, which includes permitting DHS, SSA, their contractors and other agents, upon reasonable notice, to review Forms I-9 and other employment records and to interview it and its employees regarding the Employer's use of E-Verify, and to respond in a prompt and accurate manner to DHS requests for information relating to their participation in E-Verify.

a. The Web Services Employer agrees to cooperate with DHS if DHS requests information about the Web Services Employer's interface, including requests by DHS to view the actual interface operated by the Web Services Employer as well as related business documents. The Web Services Employer agrees to demonstrate for DHS the functionality of its interface to E-Verify upon request.

23. The Web Services Employer shall not make any false or unauthorized claims or references about its participation in E-Verify on its website, in advertising materials, or other media. The Employer shall not describe its services as federally-approved, federally-certified, or federally-

recognized, or use language with a similar intent on its website or other materials provided to the public. Entering into this MOU does not mean that E-Verify endorses or authorizes your E-Verify services and any claim to that effect is false.

24. The Web Services Employer shall not state in its website or other public documents that any language used therein has been provided or approved by DHS, USCIS or the Verification Division, without first obtaining the prior written consent of DHS.

25. The Web Services Employer agrees that E-Verify trademarks and logos may be used only under license by DHS/USCIS (see [M-795 \(Web\)](#)) and, other than pursuant to the specific terms of such license, may not be used in any manner that might imply that the Employer's services, products, websites, or publications are sponsored by, endorsed by, licensed by, or affiliated with DHS, USCIS, or E-Verify.

26. The Web Services Employer agrees to complete its Web Services interface no later than six months after the date the Web Services Employer signs this MOU. E-Verify considers the interface to be complete once it has been built pursuant to the Interface Control Agreement (ICA), submitted to E-Verify for testing, and approved for system access.

27. The Web Services Employer agrees to perform sufficient maintenance on the Web Services interface in accordance with the requirements listed in the ICA. These requirements include, but are not limited to, updating the Web Services interface to ensure that any updates or enhancements are incorporated no later than six months after the issuance of an ICA. Web Services Employers should be aware that this will require the investment of time and resources. Compliance with the requirements of the ICA must be carried out to the satisfaction of DHS and or its assignees.

28. The Web Services Employer agrees that any system or interface it develops will follow the steps for creating E-Verify cases and processing tentative nonconfirmations, as laid out in the ICA, this MOU and the User Manual, including but not limited to allowing an employer to close an invalid case where appropriate, allowing an employer to refer a tentative nonconfirmation only when an employee chooses to contest a tentative nonconfirmation (no automatic referrals), and referring a tentative nonconfirmation to the appropriate agency at the time the employer prints the referral letter and provides the letter to the employee. The Web Services Employer understands that any failure to make its system or interface consistent with proper E-Verify procedures can result in DHS terminating the Web Services Employer's agreement and access.

29. The Web Services Employer understands that if it uses E-Verify procedures for any purpose other than as authorized by this MOU, the Web Services Employer may be subject to appropriate legal action and termination of its participation in E-Verify according to this MOU.

## **B. EMPLOYERS THAT ARE FEDERAL CONTRACTORS WITH THE FAR E-VERIFY CLAUSE**

NOTE: If you do not have any Federal contracts at this time, this section does not apply to your company. In the future, if you are awarded a Federal contract that contains the FAR E-Verify clause, then you must comply with each provision in this Section. See 48 C.F.R. 52.222.54 for the text of the FAR E-Verify clause and the E-Verify Supplemental Guide for Federal Contractors for complete information.

1. If the Web Services Employer is a Federal contractor with the FAR E-Verify clause subject to the employment verification terms in Subpart 22.18 of the FAR, it will become familiar with and comply with the most current version of the E-Verify User Manual for Federal Contractors as well as the E-Verify Supplemental Guide for Federal Contractors.

2. In addition to the responsibilities of every employer outlined in this MOU, the Web Services Employer understands that if it is a Federal contractor subject to the employment verification terms in Subpart 22.18 of the FAR it must verify the employment eligibility of any “employee assigned to the contract” (as defined in FAR 22.1801). Once an employee has been verified through E-Verify by the Web Services Employer, the Employer may not create a second case for the employee through E-Verify.

a. A Web Services Employer that is not enrolled in E-Verify as a Federal contractor at the time of a contract award must enroll as a Federal contractor in the E-Verify program within 30 calendar days of contract award and, within 90 days of enrollment, begin to verify employment eligibility of new hires using E-Verify. The Web Services Employer must verify those employees who are working in the United States, whether or not they are assigned to the contract. Once the Web Services Employer begins verifying new hires, such verification of new hires must be initiated within three business days after the hire date. Once enrolled in E-Verify as a Federal contractor, the Web Services Employer must begin verification of employees assigned to the contract within 90 calendar days after the date of enrollment or within 30 days of an employee’s assignment to the contract, whichever date is later.

b. Web Services Employers enrolled in E-Verify as a Federal contractor for 90 days or more at the time of a contract award must use E-Verify to begin verification of employment eligibility for new hires of the Employer who are working in the United States, whether or not assigned to the contract, within three business days after the date of hire. If the Web Services Employer is enrolled in E-Verify as a Federal contractor for 90 calendar days or less at the time of contract award, the Web Services Employer must, within 90 days of enrollment, begin to use E-Verify to initiate verification of new hires of the contractor who are working in the United States, whether or not assigned to the contract. Such verification of new hires must be initiated within three business days after the date of hire. A Web Services Employer enrolled as a Federal contractor in E-Verify must begin verification of each employee assigned to the contract within 90 calendar days after date of contract award or within 30 days after assignment to the contract, whichever is later.

c. Federal contractors that are institutions of higher education (as defined at 20 U.S.C. 1001(a)), state or local governments, governments of Federally recognized Indian tribes, or sureties performing under a takeover agreement entered into with a Federal agency under a performance bond may choose to only verify new and existing employees assigned to the Federal contract. Such Federal contractors may, however, elect to verify all new hires, and/or all existing employees hired after November 6, 1986. Web Services Employers in this category must begin verification of employees assigned to the contract within 90 calendar days after the date of enrollment or within 30 days of an employee’s assignment to the contract, whichever date is later.

d. Upon enrollment, Web Services Employers who are Federal contractors may elect to verify employment eligibility of all existing employees working in the United States who were hired after November 6, 1986, instead of verifying only those employees assigned to a covered Federal contract. After enrollment, Web Services Employers must elect to verify existing staff following DHS procedures and begin E-Verify verification of all existing employees within 180 days after the election.

e. The Web Services Employer may use a previously completed Form I-9 as the basis for creating an E-Verify case for an employee assigned to a contract as long as:

- i. That Form I-9 is complete (including the SSN) and complies with Article II.A.6,
  - ii. The employee's work authorization has not expired, and
  - iii. The Web Services Employer has reviewed the Form I-9 information either in person or in communications with the employee to ensure that the employee's Section 1, Form I-9 attestation has not changed (including, but not limited to, a lawful permanent resident alien having become a naturalized U.S. citizen).
- f. The Web Services Employer shall complete a new Form I-9 consistent with Article II.A.10 or update the previous Form I-9 to provide the necessary information if:
- i. The Web Services Employer cannot determine that Form I-9 complies with Article II.A.10,
  - ii. The employee's basis for work authorization as attested in Section 1 has expired or changed, or
  - iii. The Form I-9 contains no SSN or is otherwise incomplete.

Note: If Section 1 of Form I-9 is otherwise valid and up-to-date and the form otherwise complies with Article II.A.10, but reflects documentation (such as a U.S. passport or Form I-551) that expired after completing Form I-9, the Web Services Employer shall not require the production of additional documentation, or use the photo screening tool described in Article II.A.5, subject to any additional or superseding instructions that may be provided on this subject in the E-Verify User Manual.

g. The Web Services Employer agrees not to require a second verification using E-Verify of any assigned employee who has previously been verified as a newly hired employee under this MOU or to authorize verification of any existing employee by any Web Services Employer that is not a Federal contractor based on this Article.

3. The Web Services Employer understands that if it is a Federal contractor, its compliance with this MOU is a performance requirement under the terms of the Federal contract or subcontract, and the Web Services Employer consents to the release of information relating to compliance with its verification responsibilities under this MOU to contracting officers or other officials authorized to review the Employer's compliance with Federal contracting requirements.

### **C. RESPONSIBILITIES OF SSA**

1. SSA agrees to allow DHS to compare data provided by the Web Services Employer against SSA's database. SSA sends DHS confirmation that the data sent either matches or does not match the information in SSA's database.
2. SSA agrees to safeguard the information the Web Services Employer provides through E-Verify procedures. SSA also agrees to limit access to such information, as is appropriate by law, to individuals responsible for the verification of Social Security numbers or responsible for evaluation of E-Verify or such other persons or entities who may be authorized by SSA as governed by the Privacy Act (5 U.S.C. § 552a), the Social Security Act (42 U.S.C. 1306(a)), and SSA regulations (20 CFR Part 401).
3. SSA agrees to provide case results from its database within three Federal Government work days of the initial inquiry. E-Verify provides the information to the Web Services Employer.

4. SSA agrees to update SSA records as necessary if the employee who contests the SSA tentative nonconfirmation visits an SSA field office and provides the required evidence. If the employee visits an SSA field office within the eight Federal Government work days from the date of referral to SSA, SSA agrees to update SSA records, if appropriate, within the eight-day period unless SSA determines that more than eight days may be necessary. In such cases, SSA will provide additional instructions to the employee. If the employee does not visit SSA in the time allowed, E-Verify may provide a final nonconfirmation to the employer.

Note: If a Web Services Employer experiences technical problems, or has a policy question, the Web Services Employer should contact E-Verify at 1-888-464-4218.

#### **D. RESPONSIBILITIES OF DHS**

1. After SSA verifies the accuracy of SSA records for employees through E-Verify, DHS agrees to provide the Web Services Employer access to selected data from DHS databases to enable the Web Services Employer to conduct, to the extent authorized by this MOU:
  - a. Automated verification checks on employees by electronic means, and
  - b. Photo verification checks (when available) on employees.
2. DHS agrees to provide to the Web Services Employer appropriate assistance with operational problems that may arise during the Web Services Employer's participation in the E-Verify program. DHS agrees to provide the Web Services Employer names, titles, addresses, and telephone numbers of DHS representatives to be contacted during the E-Verify process.
3. DHS agrees to make available to the Web Services Employer at the E-Verify Web site ([www.dhs.gov/E-Verify](http://www.dhs.gov/E-Verify)) and on the E-Verify Web browser (<https://e-verify.uscis.gov/emp/>), instructional materials on E-Verify policies, procedures and requirements for both SSA and DHS, including restrictions on the use of E-Verify. DHS agrees to provide training materials on E-Verify.
4. DHS agrees to provide to the Web Services Employer a notice that indicates the Web Services Employer's participation in the E-Verify program. DHS also agrees to provide to the Web Services Employer anti-discrimination notices issued by the Office of Special Counsel for Immigration-Related Unfair Employment Practices (OSC), Civil Rights Division, U.S. Department of Justice.
5. DHS agrees to issue the Web Services Employer a user identification number and password that permits the Employer to verify information provided by its employees with DHS.
6. DHS agrees to safeguard the information provided to DHS by the Web Services Employer, and to limit access to such information to individuals responsible for the verification of employees' employment eligibility and for evaluation of the E-Verify program, or to such other persons or entities as may be authorized by applicable law. Information will be used only to verify the accuracy of Social Security Numbers and employment eligibility, to enforce the Immigration and Nationality Act (INA) and Federal criminal or anti-discrimination laws, and to administer Federal contracting requirements.
7. DHS agrees to provide a means of automated verification that is designed (in conjunction with SSA verification procedures) to provide confirmation or tentative nonconfirmation of employees' employment eligibility within three Federal Government work days of the initial inquiry.
8. DHS agrees to provide a means of secondary verification (including updating DHS records as necessary) for employees who contest DHS tentative nonconfirmations and photo non-match

tentative nonconfirmations that is designed to provide final confirmation or nonconfirmation of the employees' employment eligibility within 10 Federal Government work days of the date of referral to DHS, unless DHS determines that more than 10 days may be necessary. In such cases, DHS will provide additional verification instructions.

9. DHS agrees to provide the Web Services Employer with an Interface Control Agreement (ICA). This document will provide technical requirements that the Web Services Employer must meet to create and maintain a Web Services interface to the Verification Information System (VIS). VIS is a composite information system that provides immigration status verification for government agencies and verification of employment authorization for employers participating in E-Verify.

10. DHS agrees to provide periodic system enhancements to improve the ease and accuracy of E-Verify, as needed. DHS will also provide E-Verify enhancements to comply with applicable laws and regulations. As enhancements occur, Web Services Employers must update their Web Services interface to reflect system changes within the timelines specified in Article V.A.1. DHS will provide the Web Services Employer with an ICA to support the E-Verify release whenever system enhancements are required.

11. DHS agrees to provide to the Web Services Employer guidance on breach notification and a means by which the Web Services Employer can report any and all suspected or confirmed breaches of owned or used systems or data spills related to E-Verify cases. At this time, if the Employer encounters a suspected or confirmed breach or data spill, it should contact E-Verify at 1-888-464-4218.

12. In the event the Web Services Employer is subject to penalties, DHS will issue a Notice of Adverse Action that describes the specific violations if it intends to suspend or terminate the employer's Web Services interface access. The Web Services Employer agrees that DHS shall not be liable for any financial losses to the Web Services Employer, its employees, or any other party as a result of your account suspension or termination and agrees to hold DHS harmless from any such claims.

### **ARTICLE III**

#### **REFERRAL OF INDIVIDUALS TO SSA AND DHS**

##### **A. REFERRAL TO SSA**

1. If the Web Services Employer receives a tentative nonconfirmation issued by SSA, the Web Services Employer must print the notice and promptly provide it to the employee so that the employee may determine whether he or she will contest the tentative nonconfirmation. The Web Services Employer must review the tentative nonconfirmation with the employee in private. After the notice has been signed, the Web Services Employer must give a copy of the signed notice to the employee and attach a copy to the employee's Form I-9.

2. The Web Services Employer will refer employees to SSA field offices only as directed by the automated system based on a tentative nonconfirmation, and only after the Web Services Employer records the case verification number, reviews the input to detect any transaction errors, and determines that the employee contests the tentative nonconfirmation. The Web Services Employer will transmit the Social Security Number to SSA for verification again if this review indicates a need to do so.

The Web Services Employer will determine whether the employee contests the tentative nonconfirmation as soon as possible after the Employer receives it.

3. If the employee contests an SSA tentative nonconfirmation, the Web Services Employer will provide the employee with a system-generated referral letter and instruct the employee to visit an SSA office within eight Federal Government work days. SSA will electronically transmit the result of the referral to the Web Services Employer within 10 Federal Government work days of the referral unless it determines that more than 10 days is necessary. The Employer agrees to check the E-Verify system regularly for case updates.
4. The Web Services Employer agrees not to ask the employee to obtain a printout from the Social Security Number database (the Numident) or other written verification of the Social Security Number from the SSA.

## **B. REFERRAL TO DHS**

1. If the Web Services Employer receives a tentative nonconfirmation issued by DHS, the Web Services Employer must promptly notify employees in private of the finding and provide them with the notice and letter containing information specific to the employee's E-Verify case. The Web Services Employer also agrees to provide both the English and the translated notice and letter for employees with limited English proficiency to employees. The Web Services Employer must allow employees to contest the finding, and not take adverse action against employees if they choose to contest the finding, while their case is still pending.
2. The Web Services Employer agrees to obtain the employee's response about whether he or she will contest the tentative nonconfirmation as soon as possible after the Web Services Employer receives the tentative nonconfirmation. Only the employee may determine whether he or she will contest the tentative nonconfirmation.
3. The Web Services Employer agrees to refer individuals to DHS only when the employee chooses to contest a tentative nonconfirmation.
4. If the employee contests a tentative nonconfirmation issued by DHS, the Web Services Employer will instruct the employee to contact DHS through its toll-free hotline (as found on the referral letter) within eight Federal Government work days.
5. If the Web Services Employer finds a photo mismatch, the Web Services Employer must provide the photo mismatch tentative nonconfirmation notice and follow the instructions outlined in paragraph 1 of this section for tentative nonconfirmations, generally.
6. The Web Services Employer agrees that if an employee contests a tentative nonconfirmation based upon a photo mismatch, the Web Services Employer will send a copy of the employee's Form I-551, Form I-766, U.S. Passport, or passport card to DHS for review by:
  - a. Scanning and uploading the document, or
  - b. Sending a photocopy of the document by express mail (furnished and paid for by the employer).
7. The Web Services Employer understands that if it cannot determine whether there is a photo match/mismatch, the Employer must forward the employee's documentation to DHS as described in the preceding paragraph. The Employer agrees to resolve the case as specified by the DHS representative who will determine the photo match or mismatch.

8. DHS will electronically transmit the result of the referral to the Web Services Employer within 10 Federal Government work days of the referral unless it determines that more than 10 days is necessary.

9. While waiting for case results, the Web Services Employer agrees to check the E-Verify system regularly for case updates.

10. DHS agrees to provide the Web Services Employer with an Interface Control Agreement (ICA). This document will provide technical requirements that the Web Services Employer must meet to create and maintain a Web Services interface to the Verification Information System (VIS). VIS is a composite information system that provides immigration status verification for government agencies and verification of employment authorization for employers participating in E-Verify.

11. DHS agrees to provide periodic system enhancements to improve the ease and accuracy of E-Verify, as needed. DHS will also provide E-Verify enhancements to comply with applicable laws and regulations. As enhancements occur, Web Services Employers must update their Web Services interface to reflect system changes within the timelines specified in Article V.A.1. DHS will provide the Web Services Employer with an ICA to support the E-Verify release whenever system enhancements are required.

#### **ARTICLE IV**

#### **SERVICE PROVISIONS**

##### **A. NO SERVICE FEES**

1. SSA and DHS will not charge the Employer or the Web Services E-Verify Employer Agent for verification services performed under this MOU. The Employer is responsible for providing equipment needed to make inquiries. To access E-Verify, an Employer will need a personal computer with Internet access.

#### **ARTICLE V**

#### **SYSTEM SECURITY AND MAINTENANCE**

##### **A. DEVELOPMENT REQUIREMENTS**

1. Software developed by Web Services Employers must comply with federally-mandated information security policies and industry security standards to include but not limited to:

- a. Public Law 107-347, "E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA)," December 2002.
- b. Office of Management and Budget (OMB) Memorandum (M-10-15), "FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," April 2010.
- c. National Institute of Standards and Technology (NIST) Special Publication (SP) and Federal Information Processing Standards Publication (FIPS).
- d. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002, Information Technology — Security Techniques —

## Code of Practice for Information Security Management.

2. The Web Services Employer agrees to update its Web Services interface to the satisfaction of DHS or its assignees to reflect system enhancements within six months from the date DHS notifies the Web Services User of the system update. The Web Services User will receive notice from DHS in the form of an Interface Control Agreement (ICA). The Web Services Employer agrees to institute changes to its interface as identified in the ICA, including all functionality identified and all data elements detailed therein.
3. The Web Services Employer agrees to demonstrate progress of its efforts to update its Web Services interface if and when DHS requests such progress reports.
4. The Web Services Employer acknowledges that if its system enhancements are not completed to the satisfaction of DHS or its assignees within six months from the date DHS notifies the Web Services Employer of the system update, then the Web Services Employer's E-Verify account may be suspended, and support for previous releases of E-Verify may no longer be available to the Web Services Employer. The Web Services Employer also acknowledges that DHS may suspend its account after the six-month period has elapsed.
5. The Web Services Employer agrees to incorporate error handling logic into its development or software to accommodate and act in a timely fashion should an error code be returned.
6. The Web Services Employer agrees to complete the technical requirements testing which is confirmed upon receiving approval of test data and connectivity between the Web Services Employer and DHS.
7. DHS will not reimburse any Web Services Employer or software developer who has expended resources in the development or maintenance of a Web Services interface if that party is unable, or becomes unable, to meet any of the requirements set forth in this MOU.
8. Housing, development, infrastructure, maintenance, and testing of the Web Services applications may take place outside the United States and its territories, but testing must be conducted to ensure that the code is correct and secure.
9. If the Web Services Employer includes an electronic Form I-9 as part of its interface, then it must comply with the standards for electronic retention of Form I-9 found in 8 CFR 274a.2(e).

## **B. INFORMATION SECURITY REQUIREMENTS**

Web Services Employers performing verification services under this MOU must ensure that information that is shared between the Web Services Employer and DHS is appropriately protected comparable to the protection provided when the information is within the DHS environment [OMB Circular A-130 Appendix III].

To achieve this level of information security, the Web Services Employer agrees to institute the following procedures:

1. 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 DHS, SSA, and the Web Services Employer;

2. 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 life cycle of each organizational information system;
3. Implement subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
4. Conduct security awareness training to inform the Web Services Employer's 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;
5. Develop 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 once per year;
6. 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;
7. Implement procedures for detecting, reporting, and responding to security incidents;
8. Create plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization;
9. In information-sharing environments, the information owner is responsible for establishing the rules for appropriate use and protection of the subject information and retains that responsibility even when the information is shared with or provided to other organizations [NIST SP 800-37]].
10. DHS reserves the right to restrict Web Services calls from certain IP addresses.
11. DHS reserves the right to audit the Web Services Employer's application.
12. Web Services Employers agree to cooperate willingly with the DHS assessment of information security and privacy practices used by the company to develop and maintain the software.

### **C. DATA PROTECTION AND PRIVACY REQUIREMENTS**

1. Web Services Employers must practice proper Internet security; this means using HTTP over SSL/TLS (also known as HTTPS) when accessing DHS information resources such as E-Verify [NIST SP 800-95]. Internet security practices like this are necessary because Simple Object Access Protocol (SOAP), which provides a basic messaging framework on which Web Services can be built, allows messages to be viewed or modified by attackers as messages traverse the Internet and is not independently designed with all the necessary security protocols for E-Verify use.
2. In accordance with DHS standards, the Web Services Employer agrees to maintain physical, electronic, and procedural safeguards to appropriately protect the information shared under this MOU against loss, theft, misuse, unauthorized access, and improper disclosure, copying use, modification or deletion.
3. Any data transmission requiring encryption shall comply with the following standards:

- Products using FIPS 197 Advanced Encryption Standard (AES) algorithms with at least 256-bit encryption that has been validated under FIPS 140-2.
- NSA Type 2 or Type 1 encryption.

4. User ID Management (Set Standard): All information exchanged between the parties under this MOU will be done only through authorized Web Services Employer representatives identified above.

5. The Web Services Employer agrees to use the E-Verify browser instead of its own interface if it has not yet upgraded its interface to comply with the Federal Acquisition Regulation (FAR) system changes. In addition, Web Services Employers whose interfaces do not support the Form I-9 from 2/2/2009 or 8/7/2009 agree to use the E-Verify browser until the system upgrade is completed.

6. The Web Services Employer agrees to use the E-Verify browser instead of its own interface if it has not completed updates to its system to the satisfaction of DHS or its assignees within six months from the date DHS notifies the Web Services Employer of the system update. The Web Services Employer can resume use of its interface once it is up-to-date, unless the Web Services Employer has been suspended or terminated from continued use of the system.

#### **D. COMMUNICATIONS**

1. The Web Services Employer agrees to develop an electronic system that is not subject to any agreement or other requirement that would restrict access and use by an agency of the United States.

2. The Web Services Employer agrees to develop effective controls to ensure the integrity, accuracy and reliability of its electronic system.

3. The Web Services Employer agrees to develop an inspection and quality assurance program that regularly (at least once per year) evaluates the electronic system, and includes periodic checks of electronically stored information. The Web Services Employer agrees to share the results of its regular inspection and quality assurance program with DHS upon request.

4. The Web Services Employer agrees to develop an electronic system with the ability to produce legible copies of applicable notices, letters, and other written, photographic and graphic materials.

5. All information exchanged between the parties under this MOU will be in accordance with applicable laws, regulations, and policies, including but not limited to, information security guidelines of the sending party with respect to any information that is deemed Personally Identifiable Information (PII), including but not limited to the employee or applicant's Social Security number, alien number, date of birth, or other information that may be used to identify the individual.

6. Suspected and confirmed information security breaches must be reported to DHS according to Article V.C.1. Reporting such breaches does not relieve the Web Services Employer from further requirements as directed by state and local law. The Web Services Employer is subject to applicable state laws regarding data protection and incident reporting in addition to the requirements herein.

#### **E. SOFTWARE DEVELOPMENT RESTRICTIONS**

1. DHS reserves the right to terminate the access of any software developer [with or without notice](#) who creates or uses an interface that does not comply with E-Verify procedures.

2. Employers are prohibited from Web Services Software development unless they also create cases in E-Verify to verify their new hires' work authorization. Those pursuing software development without intending to use E-Verify are not eligible to receive an ICA. At this time, E-Verify does not permit Web Services software development without also being a Web Services Employer or Web Services E-Verify Employer Agent.

## **F. PENALTIES**

1. The Web Services Employer agrees that any failure on its part to comply with the terms of the MOU may result in account suspension, termination, or other adverse action.

2. DHS is not liable for any financial losses to Web Services Employer, its clients, or any other party as a result of account suspension or termination.

## **ARTICLE VI**

### **MODIFICATION AND TERMINATION**

#### **A. MODIFICATION**

1. This MOU is effective upon the signature of all parties and shall continue in effect for as long as the SSA and DHS operates the E-Verify program unless modified in writing by the mutual consent of all parties.

2. Any and all E-Verify system enhancements by DHS or SSA, including but not limited to E-Verify checking against additional data sources and instituting new verification policies or procedures, will be covered under this MOU and will not cause the need for a supplemental MOU that outlines these changes.

#### **B. TERMINATION**

1. The Web Services Employer may terminate this MOU and its participation in E-Verify at any time upon 30 days prior written notice to the other parties.

2. Notwithstanding Article V, part A of this MOU, DHS may terminate this MOU, and thereby the Web Services Employer's participation in E-Verify, with or without notice at any time if deemed necessary because of the requirements of law or policy, or upon a determination by SSA or DHS that there has been a breach of system integrity or security by the Web Services Employer, or a failure on the part of either party to comply with established E-Verify procedures and/or legal requirements. The Web Services Employer understands that if it is a Federal contractor, termination of this MOU by any party for any reason may negatively affect the performance of its contractual responsibilities. Similarly, the Web Services Employer understands that if it is in a state where E-Verify is mandatory, termination of this by any party MOU may negatively affect the Web Services Employer's business.

3. A Web Services Employer that is a Federal contractor may terminate this MOU when the Federal contract that requires its participation in E-Verify is terminated or completed. In such cases, the Web Services Employer must provide written notice to DHS. If the Web Services

Employer fails to provide such notice, then that Web Services Employer will remain an E-Verify participant, will remain bound by the terms of this MOU that apply to non-Federal contractor participants, and will be required to use the E-Verify procedures to verify the employment eligibility of all newly hired employees.

4. The Web Services Employer agrees that E-Verify is not liable for any losses, financial or otherwise, if the Web Services Employer or the Employer is terminated from E-Verify.

## **ARTICLE VI**

### **PARTIES**

A. Some or all SSA and DHS responsibilities under this MOU may be performed by contractor(s), and SSA and DHS may adjust verification responsibilities between each other as necessary. By separate agreement with DHS, SSA has agreed to perform its responsibilities as described in this MOU.

B. Nothing in this MOU is intended, or should be construed, to create any right or benefit, substantive or procedural, enforceable at law by any third party against the United States, its agencies, officers, or employees, or against the Web Services Employer, its agents, officers, or employees.

C. The Web Services Employer may not assign, directly or indirectly, whether by operation of law, change of control or merger, all or any part of its rights or obligations under this MOU without the prior written consent of DHS, which consent shall not be unreasonably withheld or delayed. Any attempt to sublicense, assign, or transfer any of the rights, duties, or obligations herein is void.

D. Each party shall be solely responsible for defending any claim or action against it arising out of or related to E-Verify or this MOU, whether civil or criminal, and for any liability wherefrom, including (but not limited to) any dispute between the Web Services Employer and any other person or entity regarding the applicability of Section 403(d) of IIRIRA to any action taken or allegedly taken by the Web Services Employer.

E. The Web Services Employer understands that its participation in E-Verify is not confidential information and may be disclosed as authorized or required by law and DHS or SSA policy, including but not limited to, Congressional oversight, E-Verify publicity and media inquiries, determinations of compliance with Federal contractual requirements, and responses to inquiries under the Freedom of Information Act (FOIA).

F. The individuals whose signatures appear below represent that they are authorized to enter into this MOU on behalf of the Web Services Employer and DHS respectively. The Web Services Employer understands that any inaccurate statement, representation, data or other information provided to DHS may subject the Web Services Employer, its subcontractors, its employees, or its representatives to: (1) prosecution for false statements pursuant to 18 U.S.C. 1001 and/or; (2) immediate termination of its MOU and/or; (3) possible debarment or suspension.

G. The foregoing constitutes the full agreement on this subject between DHS and the Web Services Employer.

**Approved by:**

<b>Web Services Employer</b>	
Name (Please Type or Print)	Title
Signature	Date
<b>Department of Homeland Security – Verification Division</b>	
Name (Please Type or Print)	Title
Signature	Date

**Information Required for the E-Verify  
Information relating to your Company:**

Company Name:

Company Facility Address:

Company  
Alternate  
Address  
:

County or  
Parish:

Employer Identification

Number:  
r:

North American Industry  
Classification Systems

Code:  
e:

Parent  
Company:

Number of  
Employees:

Number of Sites Verified  
for:

**Are you verifying for more than one site?**

**If yes, please provide the number of sites verified for in each State:**

State	Number of sites	Site(s)
-------	-----------------	---------

**Information relating to the Program Administrator(s) for your Company on policy questions or operational problems:**

Name:

Telephone Number:

Fax Number:

E-mail Address:

Name:

Telephone Number:

Fax Number:

E-mail Address: