E-Verify®

Supplemental Guide

For Web Services Users

December 2013

U.S. Citizenship
and Immigration
Services

TABLE OF CONTENTS

1.0 INTRODUCTION

Welcome to the 'Supplemental Guide for Web Services Users!' This guide provides information on E-Verify processes and outlines rules and responsibilities for employers and employer agents enrolled in E-Verify through a Web service. All users must follow the guidelines set forth in the E-Verify Memorandum of Understanding (MOU) and the rules and responsibilities outlined in this guide and other applicable E-Verify guidance.

For purposes of this guide, the term 'employer' means any U.S. company, corporation or business entity that is required to complete Form I-9, Employment Eligibility Verification (referred to hereafter as Form I-9) including any company employee with an E-Verify user account. In addition, the term 'E-Verify employer agent' means any U.S. company, corporation or business entity that is providing the service of verifying employees as a third party to 'clients' (employers) through the use of E-Verify. The term 'user' refers to any members of the E-Verify employer agent who are granted access to E-Verify functionality, whether through the traditional Web portal or a Web service platform.

Employers and E-Verify employer agents that use E-Verify through a Web service have chosen to develop software that interfaces with E-Verify to create cases for newly hired employees and/or certain employees of Federal Contractors with federal contracts subject to the FAR E-Verify clause.

Employers and E-Verify employer agents that use E-Verify through a Web service are held to specific requirements for the verification process in addition to requirements for development and maintenance of their interface. E-Verify employers and employer agents using Web services are required to properly train all users on E-Verify policies and procedures. The E-Verify training for Web Services will provide training requirements and guidelines for employers and E-Verify employer agents that use E-Verify through Web services to create training for their users.

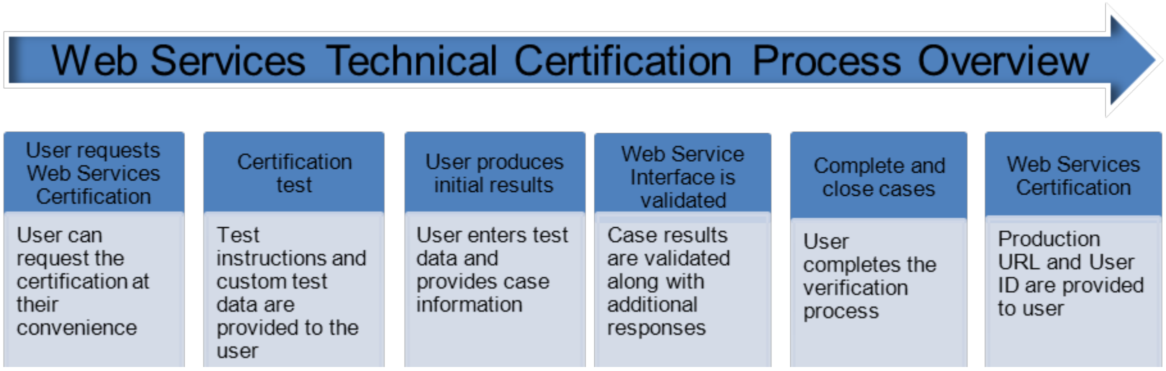
GETTING STARTED

Employers and E-Verify employer agents enroll in E-Verify by visiting the enrollment website. This website guides companies through the enrollment process. Additional information regarding enrollment is found at www.dhs.gov/E-Verify.

E-Verify provides Web Services Interface Control Agreements (ICA) to employers and E-Verify employer agents when they enroll as Web services employers or E-Verify employer agents. The ICA provides the framework for employers and E-Verify employer agents to develop an E-Verify Web service interface and contains the instructions to develop and test the software.

Several steps are required after an employer or E-Verify employer agent completes Web service development. Once development is complete, the employer or E-Verify employer agent must request a test account for the E-Verify stage environment from the E-Verify Web services support team. The timeframe for Web service activation varies and depends on the development time required by an employer's or E-Verify employer agent's developer.

The 'Web Services Technical Certification Process Overview' below provides a high-level description of the process to receive certification of the Web service interface.



Web Services Technical Certification Process Overview

User requests Web Services Certification

User can request the certification at their convenience

Certification test

Test instructions and custom test data are provided to the user

User produces initial results

User enters test data and provides case information

Web Service Interface is validated

Case results are validated along with additional responses

Complete and close cases

User completes the verification process

Web Services Certification

Production URL and User ID are provided to user

E-Verify Rules and Responsibilities

It is the employer and E-Verify employer agent's responsibility to ensure that all users understand program rules. Review these rules and responsibilities periodically with your users to ensure proper use of E-Verify and protection of employee workplace rights. Web services users must follow the guidelines below in the 'Responsibilities Overview.'

RESPONSIBLITIES OVERVIEW

Web services employers and E-Verify employer agents **MUST**:

- ✓ Upgrade their software within specified timeframes for each update or new version of E-Verify. Perform necessary maintenance on the Web services interface in accordance with ICA requirements.
- ✓ Update the company's E-Verify profile within 30 days of the Federal Contract with FAR clause award date whenever they receive notice that a client company has received such a contract.
- ✓ Notify DHS immediately if a breach of personal information occurs.
- ✓ Follow E-Verify procedures for each newly hired employee while enrolled/participating in E-Verify.
- ✓ Notify each job applicant of E-Verify participation.
- ✓ Clearly display the 'Notice of E-Verify Participation' and the 'Right to Work' posters in all languages supplied by DHS.
- ✓ Complete Form I-9 for each newly hired employee before creating a case in E-Verify.
- ✓ Obtain a Social Security number (SSN) from each newly hired employee on Form I-9, but still allow employees with a delay in receiving their SSNs to work following proper I-9 completion.
- ✓ Ensure that Form I-9 'List B' identity documents, if presented by the employee, have a photo.
- ✓ Create a case for each newly hired employee no later than the third business day after he or she starts work for pay.
- ✓ Promptly provide each employee with notice of and the opportunity to contest a tentative nonconfirmation (TNC).
- ✓ Ensure that all personally identifiable information is safeguarded.
- ✓ Not take any adverse action (e.g., reducing pay, termination, suspension, change in hours, etc.) against an employee who contests a TNC, even if it takes more than ten days for SSA or DHS to resolve the TNC.
- ✓ Contact E-Verify if you believe an employee has received a final nonconfirmation in error.

1.1 INFORMATION SECURITY REQUIREMENTS

Employers and employer agents that use E-Verify through a Web service must ensure that information they share through the Web service software and with DHS are appropriately protected through means that are comparable to security provided within the DHS environment.

The following guidance are best practices to achieve information security:

- **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 service E-Verify Employer, E-Verify employer agent and its clients.
- **Develop policies and procedures** that are based on risk assessments, reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each organizational information system.
- **Implement subordinate plans** for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate.
- **Conduct security awareness training** for Web services users, contractors and others who use the information systems to support operations and manage assets. This training informs the users of the information security risks and responsibilities associated with their activities in complying with organizational policies and procedures designed to reduce these risks.
- **Develop periodic testing** to evaluate the effectiveness of information security policies, procedures, practices, and security controls. The frequency of this testing and evaluation depends on the level of risk, but must be conducted at least once per year.
- **Develop a corrective process** sometimes referred to in quality circles as a “Corrective Action Plan.” This plan implements, evaluates and documents remedial actions addressing any deficiencies in information security policies, procedures, and practices.
- **Implement security incident procedures** for detecting, reporting, and responding sometimes referred to in security circles as a “Significant Incident Report (SIR) or Security Incident Report.”
- **Create continuity of operations (COOP) plans** and procedures to ensure ongoing operations for information systems that support the operations and assets of the organization.
- **Establish the appropriate rules for the use and protection of information**, because ultimately, the responsibility for sharing or providing information rests with the information owner.

1.2 PRIVACY BREACHES

Notify DHS immediately if a breach of personal information occurs. Breaches are defined as loss of control or unauthorized access to E-Verify personally identifiable data. All suspected or confirmed breaches should be reported by calling 1-888-464-4218 or via email at E-Verify@dhs.gov. Put “Privacy Incident-Password” in the subject line of the email sent to report the breach to E-Verify.

2.0 INTERFACE UPDATES

Employers and E-Verify employer agents using E-Verify through Web services are required to update as new versions of E-Verify become available. After the DHS system enhancement, Web service employers and E-Verify employer agents have six months from the date DHS notifies them to update their systems. The DHS notice comes in the form of an updated Interface Control Agreement (ICA) and memorandum or email. Web service E-Verify employers and E-Verify employer agents agree to institute ICA changes to their interfaces including all functionality identified and data elements.

If the Web service employer or E-Verify employer agent's system enhancements are not completed to the satisfaction of DHS or its assignees within required time period, access to E-Verify through the Web service may be denied. In addition, support for previous versions of E-Verify may no longer be available. Limited access to E-Verify via the Web browser will continue to be available.

2.1 TERMINATION

DHS has a vested interest in protecting the integrity of E-Verify. E-Verify may terminate without notice any system users who engage in behaviors resulting in security breaches, fraudulent use of the system, adverse actions against workers based upon the employer's failure to follow E-Verify rules, policies or procedures, violation of privacy laws, or other legal requirements.

DHS may also terminate without notice, the access of any Web service employer or E-Verify employer agent who creates or uses an interface that conflicts with E-Verify procedures.

Users that are federal contractors may voluntarily terminate their MOU when the federal contract that requires their participation in E-Verify is terminated or completed. See the chart below for more information.

IF…	THEN…
a federal contractor user wishes to terminate its MOU when the federal contract requiring E-Verify participation is terminated or completed,	the Web services employer or employer agent must provide written notice to DHS.
the Web services employer or employer agent does not provide written notice of its intent to terminate the MOU,	that account remains active and the E-Verify participant remains bound by the terms of the MOU that apply to non-federal contractor participants. The employer or E-Verify employer agent must continue to use E-Verify to verify employment eligibility of all newly hired employees and cannot use E-Verify to verify existing employees.

3.0 RESOURCE AND CONTACT INFORMATION

The E-Verify public website is the primary resource for all E-Verify information. For more complex questions, E-Verify may be contacted by phone or e-mail. For easy access to online resources, remember to bookmark or save the websites as 'favorites,' so future access is easier. Refer to the 'E-Verify Resources' and 'E-Verify Contact Information' charts below.

E-VERIFY RESOURCES	
E-Verify Public Website • General information about E-Verify • Program information and statistics • Frequently asked questions • E-Verify user manuals • E-Verify quick reference guides • Information about employee rights and employer obligations	www.dhs.gov/E-Verify
E-Verify Enrollment Application • Website for initial company enrollment	https://e-verify.uscis.gov/enroll

E-VERIFY CONTACT INFORMATION

E-Verify Customer Support

Questions about E-Verify? We're here to help. You can find answers to many common questions on our website at www.dhs.gov/E-Verify. In addition, we're just a phone call or email away! E-Verify Customer Support is available to assist you with using E-Verify, resetting your password and managing cases. We can also answer your questions about E-Verify policies and procedures, Form I-9 and employment eligibility. We are available Monday through Friday, from 8 a.m. Eastern Time through 5 p.m. Pacific Time, except on federal holidays.

For Employers:	888-464-4218 877-875-6028 (TTY) E-Verify@dhs.gov
For Employees:	888-897-7781 877-875-6028 (TTY) E-Verify@dhs.gov

Our normal response time for e-mail inquiries is two business days. If we need more time to respond, we'll contact you within two business days to explain why we need additional time and provide you with an estimated response time.

Office of Special Counsel for Immigration-Related Unfair Employment Practices (OSC)

OSC is available to answer your questions about immigration-related employment discrimination, including discrimination based on citizenship status, immigration status or national origin in the Form I-9 and E-Verify processes. OSC's website has helpful (and downloadable) guidance to assist employers in avoiding employment discrimination while using E-Verify and completing the Form I-9.

Employer Hotline:	800-255-8155 800-237-2515 (TTY)
Employee Hotline:	800-255-7688 800-237-2515 (TTY)
Website:	http://www.justice.gov/crt/about/osc
Email:	osccrt@usdoj.gov