Electronic I-9 Documentation

Guardian Electronic I-9 and E-Verify Compliance with 8 CFR 274a.2

Abstract

This document may be provided to Immigration and Customs Enforcement (ICE) in connection with a Form I-9 Notice of Inspection involving I-9s electronically generated and/or stored in the Guardian Electronic I-9 and E-Verify System.

Copyright Hyland Software, Inc. 2018
# Table of Contents

Name of Electronic I-9 Software and Vendor ........................................................................................................... 3
Internal Business Practices and Protocols .................................................................................................................. 3
Indexing System ......................................................................................................................................................... 4
Electronic Signature Compliance ............................................................................................................................... 5
Audit Trail Compliance ............................................................................................................................................. 10
Guide to Reviewing the Guardian Electronic I-9 and E-Verify Audit Trail ................................................................. 11
Name of Electronic I-9 Software and Vendor

This document pertains to the Guardian Electronic I-9 and E-Verify application (“Guardian”), a comprehensive compliance solution designed and maintained by the LawLogix Division of Hyland Software, Inc. Guardian is one of the most widely used electronic I-9 and E-Verify applications on the market today, serving organizations throughout the US in various industries and locations. Guardian was first developed in 2006 by in-house immigration attorneys, with a particular focus on satisfying the ICE regulations for electronic signature and storage of Forms I-9. Since that time, Guardian has continued to make advances in employment eligibility verification while always ensuring that the software meets the required electronic safeguarding and security standards as described in more detail below.

For more information on Guardian and LawLogix, please visit http://www.lawlogix.com. Questions regarding this document or Guardian’s compliance with the electronic I-9 regulations may be directed to:

John Fay
LawLogix, VP and General Counsel
jfay@lawlogix.com

Internal Business Practices and Protocols

The Guardian Electronic I-9 system by LawLogix meets the following criteria established by 75 FR 42575-42579 and codified at 8 C.F.R. §274a.2(e):

1. Processes and Controls to ensure the integrity, accuracy and reliability of the electronic storage system

   The Guardian electronic I-9 storage system is maintained in a secure environment which utilizes the latest in data protection technology to ensure the integrity, accuracy and reliability of all I-9 data. Access to this facility is controlled by biometric authentication, swipe card validation, sign-in logs and 24-hour video monitoring. All of the hardware (servers, routers, backup devices, etc.) related to the electronic I-9 computing environment is exclusively managed by LawLogix. In addition, the Guardian solution features the following security safeguards:

   - LawLogix’s cyber threat resistant architecture contains multiple UNIX server clusters which are hosted at a Tier 3 Co-location facility (multiple power and cooling sources, though only one is active at a time and uptime of 99.982%) in seismically neutral, non-flood, non-fire risk location in Arizona. All client personally identifiable information (i.e. Social security number, date of birth, etc.) is encrypted “at rest” utilizing 256-bit AES.

   - All I-9 data sent through the system is encrypted “in transit” with Symantec Class 3 SSL Certificates using at least 128-bit Encryption utilizing SSLv3/TLSv1.

   - LawLogix utilizes best-in-class firewall and server technology, strong SSL encryption, vulnerability scanning and a Network Intrusion Detection/Prevention System that proactively monitors and prevents malicious attacks.

   - LawLogix contracts with a security expert to conduct an annual evaluation of the Guardian system and LawLogix practices.

2. Reasonable controls designed to prevent and detect the unauthorized or accidental creation of, addition to, alteration of, deletion of, or deterioration of an electronically completed or stored Form I-9, including the electronic signature if used
Access to the Guardian system requires a unique user login and complex password in order to ensure the integrity, safety, and privacy of the I-9 and E-Verify data. All new users must be granted specific privileges in order to perform various actions in the system, including completing an I-9, approving an I-9, and accessing the E-Verify system. In addition, Guardian also grants permission by security groups, user-defined classes, and actual employer locations to enable employers to effectively mimic their organization hierarchy and adhere to a “least-access” or “need to know” security approach.

On the technical side, Guardian employs a 3-point security checkpoint system in which user rights and company associations are checked at the point of querying the database, at the point of saving data to the database, and at the point of preparing the web page for viewing by the user. All actions related to the I-9 process are recorded in a detailed audit trail (further explained below), and all user logins and authentications are tracked in a detailed activity log.

3. An inspection and quality assurance program that regularly evaluates the electronic generation or storage system, and includes periodic checks of electronically stored Forms I-9, including the electronic signature.

LawLogix maintains a detailed Quality Assurance/Software Test Plan which calls for regular evaluation of the Guardian Electronic I-9 and E-Verify system. Specifically, LawLogix will conduct planned system audits and evaluations to ensure that the system is operating as designed, and Forms I-9 are being created, saved, and maintained for retrieval as required under the regulations. As part of this evaluation, LawLogix will also ensure that all required data backups are being properly saved. In the case of a new Guardian feature, LawLogix will conduct “regression testing” to determine whether a change in one part of the software affects other elements of Guardian, with a particular focus on the electronic generation, storage and signing of I-9 forms.

4. Produce a high degree of legibility and readability when displayed on a video display terminal or reproduced on paper.

All I-9s in the Guardian system can be viewed in Adobe PDF, which provides a high degree of legibility and readability on both a computer/mobile screen and printed copy. In addition, all supporting documents which are scanned into Guardian can also be easily viewed and printed.

Indexing System

The Guardian electronic system features a detailed indexing scheme that consists of both employee records and associated I-9 records which can be searched and retrieved by the following criteria:

- Employee name
- Location name, city, and state
- Employee ID number (if available)
- Social Security Number
- Date hired or terminated
- Responsible HR or HR Group
- Business unit
- Employee status
- I-9 status
- Other custom-defined attributes
Electronic Signature Compliance

The Guardian electronic I-9 signature process was designed to meet the most conservative interpretation of the regulations published at 75 Fed. Reg. 42575 (Jul. 22, 2010) and codified at 8 C.F.R. § 274a. In particular, these standards prescribe certain controls which must exist in the electronic I-9 system to maintain the integrity of the I-9 records and to demonstrate the trustworthiness of the process that created and preserved the records in question. The key requirements for a valid employee electronic I-9 signature are as follows:

1. The system used to capture the electronic signature must include a method to acknowledge that the attestation to be signed has been read by the signatory
2. The electronic signature must be attached to, or logically associated with, an electronically completed Form I-9
3. The system must affix the electronic signature at the time of the transaction
4. The system must create and preserve a record verifying the identity of the person producing the signature
5. Upon request of the employee, the system must provide a printed confirmation of the transaction to the person providing the signature

With respect to electronic signatures for employers or representatives, the system should include a method to acknowledge that the attestation to be signed has been read by the signatory.

The LawLogix System: Guardian’s Multi-Step Electronic Signature Process

The Guardian Electronic I-9 and E-Verify signature process for employees satisfies each of the regulatory requirements as follows:

Legal Requirement #1: “The system used to capture the electronic signature must include a method to acknowledge that the attestation to be signed has been read by the signatory.”

Guardian I-9: Guardian’s electronic signature technology employs a multi-step electronic signature acknowledgement and verification process whereby the employee needs to type his/her name and verify that he/she is the person signing the form; confirm his/her identity through three (3) biographic points of data, including first name, last name, and date of birth; acknowledge the Form I-9 attestations and certifications through a “Click to Accept” mechanism; and provide either a pin number or an answer to a question (from a pre-defined list) which calls for information that only the employee would reasonably know.

The following illustrations depict the electronic signature process for a new hire employee in Guardian through the signature question-answer process.

Figure 1. Employer launches the employee workflow
Figure 2. Employee confirms identity

Employee Identity

You are being asked to complete Section 1 of the Form I-9. Please provide your legal name below. This information will be used to identify who completed Section 1 of the form.

Employee Name
(First and Last)  Edward Employee

I confirm that I am the employee named above.

Cancel  Continue as Employee

Figure 3. Employee electronic signature and verification

Electronic Signature

You, the employee, must sign Section 1 as described below. By signing this form, you attest under penalty of perjury that the information you provided, along with the citizenship or immigration status you selected, and all information and documentation you provide to your employer, is complete, true and correct, and you are aware that you face severe penalties provided by law and may be subject to criminal prosecution for knowingly or willfully making false statements or using false documentation when completing this form.

Step 1: Please verify that the first name, last name, and date of birth shown below belong to you by clicking the checkbox next to each item.

- First Name  Edward
- Last Name  Employee
- Date Of Birth  12/13/1978

Step 2: Read the following statement and select "I Accept" to acknowledge your agreement:

I consent to provide an electronic signature in connection with this Form I-9 and understand that by verifying my name and date of birth in Step 1 above, providing the requested information in Step 3 below, clicking on the ‘I Accept’ box, and clicking on the ‘Electronically Sign’ button, that I am electronically signing this Form I-9. I understand that my electronic signature will be binding as though I had physically signed this document by hand.

- I Accept

Step 3: Please select a signature question from the dropdown list, provide an answer, and click ‘Electronically Sign’ to complete your electronic signature. The question selected should call for information that you have committed to long-term memory and is not easily guessed or researched. Please note that the question and answer may be presented to the Department of Homeland Security in the event of an audit as proof that you have electronically signed this document.

Question:  What is the name of the hospital where you were born?
Answer:  Newtown Square General Hospital

Electronically Sign
Figure 4. Employee completes section 1 process

The following message will display to an employee who is completing section 1 of the electronic I-9 in the physical presence of the employer representative (“I-9 Verifier”). If section 1 was completed by the new hire employee on his or her own computer, the message would simply instruct the employee to close the window and meet with the employer to provide original documents.

Legal Requirement #2: “The electronic signature must be attached to, or logically associated with, an electronically completed Form I-9.”

Guardian I-9: Once an I-9 has been electronically signed, Guardian stores and associates the electronic signature with the employee’s I-9 record, as represented in the Guardian audit trail, software user interface, and the resulting “hardcopy” Form I-9.

Figure 5. Guardian user interface showing electronic signature for completed I-9

Figure 6. Final “hardcopy” I-9 with electronic signature in section 1
Legal Requirement #3: “The system must affix the electronic signature at the time of the transaction”

Guardian I-9: As illustrated in Figure 5 above, Guardian automatically records the precise date and time when the signature is initiated in the Guardian system.

Legal Requirement #4: “The system must create and preserve a record verifying the identity of the person producing the signature”

Guardian I-9: When an I-9 is electronically signed, the Guardian system records the electronic signature in an immutable audit trail record, which identifies the person producing the signature and the date/time it was initiated.

Figure 6. Audit Trail of Section 1 highlighting electronic signature

Legal Requirement #5: “Upon request of the employee, the system must provide a printed confirmation of the transaction to the person providing the signature.”

Guardian I-9: The Guardian I-9 system can generate a printable receipt of the employee’s electronic signature, which includes a summary of the attestation, employer name, employee name, and the date/time the signature was completed.

Figure 7. Confirmation of Employee Section 1 Electronic Signature
Lastly with respect to electronic signatures in sections 2 or 3 of the Form I-9, the Guardian system requires the employer or employer’s representative to read the required attestation, click to “accept,” and provide a unique individual password before electronically signing the form.

**Figure 8. Section 2 Electronic Confirmation and Signature**

![Electronic Signature](image)

*The remainder of this page left intentionally blank. Please proceed to page 10.*
Audit Trail Compliance

The Guardian electronic I-9 system maintains a comprehensive and immutable audit trail that records whenever an electronic Form I-9 record is created, completed, updated, modified, altered or corrected. The flowchart below depicts when audit trail records are created in the Guardian system throughout a typical Form I-9 workflow.

I-9 Created

- Employer Login
- Employer initiates I-9 in Guardian which is associated (indexed) with new hire record

Section 1 Completed

- New hire completes section 1, providing personal information and attestation
- New hire electronically signs section 1, and Guardian creates a record verifying the identity of the person
- Preparer/translator certification completed (if applicable)

Section 2 Completed

- Employer accesses section 2
- Employer selects documents presented (either List A or a combination of List B and List C)
- Employer enters document information, start date, & business information
- Employer electronically signs section 2 with unique password or identifier

I-9 Updated (section 3)

- Employer adds a section 3 to the I-9
- Employer records additional information in section 3 (name, documents, etc.)
- Employer electronically signs section 3 with unique password or identifier

I-9 Modified, Altered, or Corrected

- Employer adds an amendment to section 1, 2, or 3
- Employee or employer inserts new or corrected information
- Employee or employer electronically signs the amendment
Guide to Reviewing the Guardian Electronic I-9 and E-Verify Audit Trail

Audit Trail Header

**Date & Time:** displays the date and timestamp when the I-9 information was “created” in Guardian. Per the regulations, the system also creates audit trail records when the I-9 is completed, updated, modified, altered, or corrected.

**Type:** this is an internal database designation to indicate whether the record was added or updated.

**User:** displays the logged in user in the Guardian system when the I-9 changes were made. Note that this may be the HR or hiring representative who initiated the I-9 process and handed the keyboard over to the new hire.

**Button or Action:** this may be either the button clicked or a particular action which has occurred during the audit trail event period. For example, a “Check Form” action indicates that the employee or employer has saved the data, and Guardian is checking for errors. If the action indicates “[more],” this simply means that the Guardian system is creating data relationships behind the scenes (i.e., between I-9 records and employee records or employee records and associated locations).

Snapshot of Audit Trail Header

```
Audit for i9 - page 1 (Jones, John)

| Audit # | Date & Time | TYPE | User | (Button) or [Action] |
```

Audit Trail Event

Each audit trail event will capture changes made to the I-9 record, including the new data and prior data (if any). The first audit trail event will typically record the creation of the I-9 record by the employer representative. It’s important to note that many of the fields will be blank at this point, since the new hire has not yet completed section 1.

Please note that individual audit trails may vary slightly depending upon when the I-9 was generated and how the employee accesses section 1. The following pages depict a typical audit trail in Guardian for a Form I-9 where section 1 was completed “in-person” with the employer representative using the same computer.

Audit Trail event #1 depicts the I-9 record being created by an HR Manager for employee John Jones on February 19, 2018. Each I-9 record in Guardian has a unique “key” which can be used by the employer to retrieve specific records.

```
Table: i9, Key: 231111

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>l</td>
<td>02/19/2018 06:18:21</td>
<td>231111</td>
<td>Smith, Stephanie</td>
<td>Jones, John</td>
</tr>
<tr>
<td></td>
<td>'key'</td>
<td>'emp key'</td>
<td>'com key'</td>
<td>'dt created'</td>
</tr>
<tr>
<td></td>
<td>{}</td>
<td>874077</td>
<td>32</td>
<td>02/19/2018 06:18:20.910628</td>
</tr>
</tbody>
</table>
```
Audit trail event #3 shows that the Form I-9 has been accessed by the new hire (John Jones) through the Guardian interface. This step occurs immediately before the new hire is presented with the section 1 fields and questions.

Audit trail event #4 depicts the employee providing section 1 data, including names, address, date of birth, social security number, and attestation. All of the prior values are listed as “none” since this is the first time that the employee is providing this information on the form.

Audit trail events #5 and #6 show the new hire employee electronically signing section 1 and providing a unique question and answer response to help verify that he was the individual signing the form. For security purposes, the answer depicted below is only available through the exported audit trail (and not viewable within the system). The Guardian system also electronically associates the electronic signature with the employee’s I-9 record through the employee’s unique I9 key (231111 below) and keeps track of the first time that a section 1 is signed (important, in the event an employee later makes changes and re-signs the form).
Audit trail events #7 and #8 show the employer representative accessing section 2 of the employee’s I-9 record in Guardian. Certain pieces of employer data are automatically inserted into section 2 based on the logged-in employer user, including the individual’s name, title, business name, and address.

Audit trail events #9 and #10 depict the employer representative selecting a ‘List A’ U.S. Passport from the drop-down menu in section 2 of the form and entering the document issuing authority, number, and expiration date. Audit trail #10 also shows the employer entering the new hire’s first day of work for pay. Please note that the number “55” in audit trail event #9 below is an internal Guardian document identifier.

Audit trail event #12 depicts the I-9 due date (an internal I-9 management field), which is calculated as three business days after the new hire’s first day of employment.

Audit trail event #13 depicts the employer representative electronically signing section 2 using a unique password or identifier.

Lastly, audit trail events #15 and 16 show when the I-9 was marked “completed” and “approved” in Guardian. It’s important to note that these are merely internal I-9 workflow “stages” which are designed to facilitate the employer’s review of the I-9. From a compliance standpoint, the I-9 is fully completed as of the date the section 2 is signed.