

use the information contained in CTMS or compiled by compliance analysts to support a state enforcement case against an employer. Depending upon the jurisdiction, this could result in loss of a business license, loss of a state contract, fine or other severe penalties.

E-Verify Violations Can Result in a Variety of Outcomes for Employers

When USCIS analysts determine that non-compliant activities or violations are occurring, this determination can result in a range of outcomes for employers. These outcomes include remediation by the employer; additional training on E-Verify; suspension from E-Verify; referral to the Office of Special Counsel for Immigration-Related Unfair Practices (OSC) at the Department of Justice; and referral to a law enforcement agency, including Immigration and Customs Enforcement (ICE). USCIS does not have the ability to bring federal enforcement actions on its own; however, it could work with ICE or other agencies to bring a case against an employer.

USCIS Will Keep the E-Verify Related Information For Ten Years

The federal register notices and PIA provide that the information gathered by the system will be maintained for a period of ten years, or longer if needed by law enforcement or for another investigation. Accordingly, employers should consider whether their document retention policies regarding E-Verify and I-9 documents protect them for this entire time period.

Employers on E-Verify Should Adopt Rigorous Compliance Procedures

Employers join E-Verify for a variety of reasons. Some employers join E-Verify with the best of intentions and aspire to serve as a model of compliance. Some join to try to mitigate the effects of a pending law enforcement action. Some join because they are forced to do so. Regardless of an employer's initial motive, once they join E-Verify, they often assume E-Verify implementation is running smoothly. It appears rare that employers audit their system, or that they provide regular training to E-Verify users. Given the current environment, and recent federal register notices and PIA, this is a mistake. Employers should adopt rigorous compliance procedures to ensure appropriate E-Verify participation and avoid government scrutiny.

Best practices in this area include:

- Providing standardized ongoing training for all E-Verify users;
- Providing core I-9 training for all E-Verify users;
- Organizing E-Verify as part of the I-9 process rather than housing it elsewhere;

- Sharing E-Verify basic compliance manual with all E-Verify users;
- Tasking an authorized employee to run reports on E-Verify use on a regular basis to observe any trends and patterns, as well as to ensure all cases are resolved appropriately;
- Ensuring that the Administrator reviews such reports and then provides them to an individual or team who is not otherwise involved with E-Verify operations;
- Considering self-reporting when appropriate;
- Having outside auditors and legal counsel review the process to assess exposure and concerns;
- Establishing and maintaining safeguards to prevent use of the E-Verify process for unlawful discrimination;
- Creating and implementing standardized protocol when USCIS's Verification Division contacts the employer, involving immediate company-wide attention, referral to legal counsel, and focus on potential problems;
- Abiding by appropriate document retention policies; and
- Conducting annual I-9 and integrated E-Verify internal audits.

Conclusion

While E-Verify is still the right choice for most employers, it is not a panacea for all compliance concerns. Now, more than ever, employers cannot simply join E-Verify and then forget about immigration compliance obligations. E-Verify participation never insulated employers from ICE investigation, but in the past it did not trigger ICE worksite actions. Depending on how CTMS is eventually implemented and utilized, it is possible that E-Verify usage could become a new source for ICE and OSC leads. Rigorous compliance protocols for E-Verify are essential to avoid problems and increasing government scrutiny contemplated by CTMS.

Links to the USCIS CTMS Documents Referenced In This Article:

<http://edocket.access.gpo.gov/2009/E9-11966.htm>

<http://edocket.access.gpo.gov/2009/E9-11967.htm>

http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_ctms.pdf

**** The information provided above does not constitute legal advice and no attorney-client relationship is created by this generalized information. For specific guidance, please contact ICS or legal counsel. ****



www.iandcsolutions.com

1-888-885-6650



E-Verify Employers Should Prepare For USCIS's Announced Increase in Monitoring

By Julie Myers Wood
June 2009

www.iandcsolutions.com
1-888-885-6650

E-Verify Employers Should Prepare For USCIS's Announced Increase in Monitoring

E-Verify is a critical tool for employers who want to prevent hiring unauthorized workers. And yet, employers who voluntarily sign up for E-Verify often wonder what happens to the information that they provide to the E-Verify system, and whether their activities are subject to additional scrutiny because of their participation. U.S. Citizenship and Immigration Service (USCIS) recently provided a clear, if unsatisfying, answer: the information employers provide to these systems is being scrutinized now and USCIS plans to analyze this information even more closely in the future.

Although the new monitoring announced by USCIS is a reasonable cause for employer concern, employers should not let it deter them from joining E-Verify. Instead, the new scrutiny should provide an incentive for employers to consider all of the implications involved in joining E-Verify, and develop a basic and workable E-Verify compliance system, which carefully considers the anti-discrimination laws, as well as I-9 procedures.

USCIS announced the enhanced monitoring in its recently published Systems of Records Notice (SORN), Privacy Act Exemption Notice, and a Privacy Impact Assessment (PIA) for a new system to monitor E-Verify called the Compliance Tracking and Management System (CTMS). USCIS published these documents as required by law before the agency could start using the CTMS system. (USCIS is accepting comments on the SORN and Privacy Act Exemption Notice until June 22, 2009, and proposes to start using the system on June 22, 2009.)

The new CTMS notices should spark interest and comment from the more than 120,000 employers who voluntarily participate in the E-Verify system. Although USCIS's increased compliance and monitoring should not come as a surprise, some employers may not have previously fully focused on the responsibilities that come with participation in E-Verify. The E-Verify memorandum of understanding and standard training module also do not provide adequate information or guidance to employers on what is required to ensure that there is no abuse, fraud or misuse of the program.

USCIS officials have stated that the intent of the new CTMS system is to assist employers and alert them of potential issues and misuse in a positive way. However, employers must be aware that information provided or gathered by USCIS may be shared with law enforcement agencies and could be used in a case against an employer. As such, the CTMS notices and PIA provide guidance and a roadmap for where USCIS is going in terms of E-Verify use and tracking, and how those changes will affect employers. E-Verify employers should take steps now to ensure that they are fully compliant with the system to avoid intrusive government oversight and costly mistakes.

USCIS Is Increasing Its Monitoring of the E-Verify System

As explained in the notices and PIA, USCIS's Verification Division will operate the Compliance Tracking and Monitoring System (CTMS) as part of its efforts to monitor E-Verify. USCIS describes CTMS as a "new system" that collects and uses information necessary to support monitoring and compliance activities for researching and managing misuse, abuse, discrimination, breach of privacy, and fraudulent use of E-Verify. USCIS monitoring and compliance analysts will use the CTMS and provide the information obtained from the system to various individuals and agencies.

The notices and PIA make clear that CTMS is developing "detailed procedures" for monitoring verification and performing compliance activities of E-Verify. These procedures and tracking modules, which will be developed over time, will at first use existing and new consumer-off-the-shelf software products, but later may use additional and more sophisticated analytic and information management tools.

E-Verify Monitoring Will Focus on Particular Employer Activities

USCIS will use CTMS to support a wide range of monitoring and compliance efforts relating to employer activities. These efforts will include but not be limited to, efforts regarding:

- Fraudulent use of Alien numbers (A-Numbers) and SSNs by E-Verify users;
- Termination of an employee because of a tentative non-confirmation (TNC);
- Verification of wrong categories of individuals
 - o Applicants instead of new employees (pre-screening),
 - o Some employees rather than all, or
 - o Other sorts of selective screening issues;
- Failure to notify DHS when an employee who receives a final non-confirmation (FNC) is not terminated;
- Failure to post the notice informing employees of participation in E-Verify; and
- Failure to use E-Verify consistently, or at all, once registered.

Given that USCIS has specifically identified each of these areas, employers should ensure that they make each of these areas a core part of their regularized training and compliance systems for E-Verify.

USCIS Monitoring and Compliance Analysts Will Investigate E-Verify Violations

USCIS's Verification Division will obtain information about potential non-compliant activities or E-Verify violations by monitoring transactions on the E-Verify system. USCIS will also use tips, information from law enforcement agencies, and the media.

To aid in their investigation of potential violations, USCIS is establishing thresholds to narrow their research to find the most likely cases of non-compliant behaviors. Once the monitoring analysts determine that a particular behavior meets the threshold established by USCIS, the compliance analyst may begin researching the behavior.

The research conducted by the compliance analyst will vary, but generally USCIS states the first step is contacting or visiting the E-Verify user to notify them that they may not be in compliance with program requirements. USCIS states that this contact will allow the E-Verify user to explain or remediate the behavior. Obviously, it is in the employer's interest to fully resolve the matter at this stage whenever possible. If USCIS does not appear satisfied with the employer's attempt to resolve the matter, the employer should consult with compliance experts or counsel, and consider taking additional steps to talk with an USCIS supervisor in order to get the matter resolved satisfactorily.

Resolving compliance inquiries at this initial stage is critically important because if USCIS believes that the E-Verify user is unable to adequately explain or remediate the behavior, compliance analysts may conduct additional, potentially burdensome inquiries.

In conducting the additional inquiries, compliance analysts may:

- Conduct Interviews of Individuals at Employer who Use E-Verify (Human Resources, Office Managers, Others);
- Collect E-Verify created documents;
- Collect Tentative Non-Confirmation letters;
- Collect Referral Letters;
- Collect I-9 Forms;
- Collect Supporting Documentation for I-9s;
- Collect Employment Offer Letters; and
- Collect Termination Letters.

This list is not exhaustive, and employers should be prepared to have a wide range of requests come from particular compliance analysts. It is also not clear what legal authority USCIS has to gather the additional documents and testimony. If there is

a question about a particular record sought, employers should consider checking with their legal counsel to seek the basis for production of the documents. However, as a practical matter, refusal to provide some of the documents requested by USCIS could prompt quick interest (or subpoenas) from U.S. Immigration and Customs Enforcement, so it is wise to tread lightly and think through this process very carefully. With respect to interviews, employers may find that there are situations where interviews would provide problematic information. In such a situation, it is imperative that the employer seek advice of legal counsel before consenting to an interview.

The burden and focus is on the employer. It is significant that the PIA states that CTMS compliance operations, such as interviews or document requests, will be focused "directly on the users of the systems – the employers. . . , rather than on the individuals who are being verified." In other words, despite the rampant identity fraud often committed by undocumented employees at E-Verify companies, USCIS will not address this issue with the employees providing the fraudulent documents – instead, USCIS will question the employer to see whether the employer took all appropriate steps to spot repeat Social Security numbers and prevent abuse.

USCIS May Provide the Information It Collects To All Appropriate Authorities

Employers should note that the federal register notices and PIA do not give any assurance to employers that the information collected from their voluntary participation in E-Verify will be used solely to bring the employer into compliance with E-Verify. USCIS officials have indicated that they plan to use the information for compliance purposes, but nothing in the CTMS notices restricts the use for compliance purposes only.

In particular, the CTMS notices provide that the information collected by the compliance analysts will be kept confidential, except when the information must be released by "legal necessity." This phrase is hardly reassuring to employers who are trying in good faith to comply with E-Verify procedures, but who face a problem of identity theft in their workforce or other issues with E-Verify compliance. Is legal necessity a request by an ICE agent? Is legal necessity a suspicion by a compliance analyst that a company has not run E-Verify on all employees? In the absence of clarity, employers should assume that legal necessity is whatever USCIS analysts determine it to be in any particular situation.

Moreover, employers should be aware that information obtained by USCIS compliance analysts could be shared, not only with law enforcement within DHS, but also with other appropriate Federal, State, local, Tribal, foreign, or international government agencies. It is easy to imagine a scenario where state government agencies requiring participation in E-Verify