APRIL 3, 2013 ISSUE NO. 745

HR Compliance Library

Ideas & Trends

INSIDE THIS ISSUE

Wolters Kluwer
Law & Business

wolterskluwerlb.com

CYBER SECURITY

Employers have yet to take document and cyber security seriously enough, says expert

Over 75 percent of U.S. business valuation is comprised of intangible assets, which are largely electronically stored, according to Keith Chval, attorney and co-founder of Protek International, a computer forensics, investigations and litigation support firm (www.protekintl.com). And, the Department of Commerce estimates that U.S. companies lose between $200 and $250 billion each year to Intellectual Property theft. "These facts make it hard to over-state the concern that employers should have over cyber security," Chval said in an interview with Wolters Kluwer Law & Business.

"Surely there's been improvement since I first began beating the cyber security drum at various trade group and association meetings over 15 years ago," said Chval, "but there's still a whole lot of room for improvement. There are surely exceptions to every rule, but as a whole, employers are not yet taking the issue seriously enough."

continued on page 28

EMPLOYEE PERFORMANCE

PIPs are valuable employer tools when used correctly

Performance improvement plan: (a) valuable tool for correcting performance problems, or (b) obligatory pre-discharge formality? If you answered (a), you know that a PIP can help a faltering employee meet job expectations — an important goal given the costs of employee training and turnover. If you answered (b), try again.

In most states, a PIP is not a legal prerequisite to termination because employment is generally "at-will," meaning that either side can terminate the employment relationship for a good reason, a bad reason, or no reason at all, but not for an unlawful reason (such as discrimination or in retaliation for whistleblowing). Nevertheless, for many private-sector employers, the PIP serves a genuine "due process" function of sorts, a fair warning and last chance for an employee to avoid discharge. But when a PIP is used for the sake

continued on page 30

CYBER SECURITY

continued from page 27

Reports confirm what Chval already knows. On January 24, 2013, PwC US revealed its *2013 Top 10 Technology Trends for Business* report, which highlights the most significant trends in technology affecting organizations for the upcoming year. Second only to "pervasive computing" (the ability to digitally engage and interact via mobile devices with enabled objects around you) the top technology trend for businesses in 2013 is Cyber Security.

> *"It's no longer a discussion about if an organization will get hacked, but only a matter of when, and how quickly and effectively it will respond."*

A February, 2013 study conducted by Deloitte Consulting, LLP, further confirms Chval's thought that there is room for improvement in organizations' cyber security efforts. Twenty eight percent of study participants reported that their organization was the victim of at least one cyberattack during 2012; 9 percent report multiple breaches; and 17 percent were not confident that their organization could even detect an attack.

"It's no longer a discussion about if an organization will get hacked, but only a matter of when, and how quickly and effectively it will respond," said Mark White, principal and chief technology officer, Deloitte Consulting LLP. "Organizations across many industries need to change the lens through which they view cyber risk – not only relying on traditional security controls to reveal tell-tale signs of an effective attack — but by considering transforming the way they defend, detect and even manage security by leveraging cyber intelligence and advanced techniques to help identify the coming threat and proactively respond."

Defining cyber security at work

It really is naïve to assume that "cyber security" merely includes protecting an employee's pay information, performance review, or social security number. Chval explains that the definition of "cyber security" goes much, much deeper than that.

"There's virtually nothing within an organization today that's not susceptible to some flavor of cyber malfeasance," he says. "Certainly privacy issues with respect to employees' and others' personal information held within the enterprise's systems is a significant cyber security issue. Beyond that, the term extends to critical facets of an enterprise's lifeblood to include electronically stored Intellectual Property, on-line commerce operations, critical IT and communications infrastructure, and access to financial assets, just to name a few."

Who is responsible for cyber security at work? "It's easy to say that employers owe employees cyber security at work, but that really is a two-way street," said Chval. "Of course employers need to protect employees' personal information, as well as the enterprise's well-being to ensure its continued vitality and the employees' livelihoods, but employees also owe it to the employer and their fellow employees for those very same reasons."

In the end, Chval says, cyber security at work is everyone's responsibility. "Depending on the size and resources of an employer, specific individuals are typically tasked with cyber security responsibilities, either in whole or in parts thereof," he explained. "Individuals with these job responsibilities might be found within the IT department, security, or some variation thereof. But, to have any hope of a reasonable level of cyber security, literally every employee needs to consider it a responsibility."

Engaging in cyber security practices

Chval points to study after study suggesting that Insiders (*e.g.*, employees, maintenance personnel, executives, assistants, etc.) are the biggest threat to an employer's cyber

continued on page 29

HR Compliance Library
Ideas & Trends

Managing Editor: Heidi J. Henson, J.D.

Contributing Editors: Cynthia L. Hackerott, J.D. Joy Waltemath, J.D.

Newsletter Design: Kathie Luzod

Newsletter Layout: Chris Tankiewicz

HR COMPLIANCE LIBRARY—Ideas & Trends (USPS 680-810)(ISSN 0745-0613), a Wolters Kluwer editorial staff publication, is published monthly by Wolters Kluwer, 4025 W. Peterson Ave., Chicago, Illinois 60646. Periodicals postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO HR COMPLIANCE LIBRARY—IDEAS & TRENDS, 4025 W. PETERSON AVE., CHICAGO, IL 60646. Printed in U.S.A.

CYBER SECURITY

continued from page 28

security. "That might be from the employee who sets out to victimize her employer or her fellow employees or the individual who inadvertently creates cyber security vulnerabilities and incidents," explained Chval.

As a result, Chval recommends that employers develop and implement a "reasonable, effective cyber security plan that not only identifies and secures critical information and assets, but also takes into account the organization's culture to ensure maximum employee buy-in."

> *"I really don't think you can overestimate the value of employee education and awareness when it comes to cyber security. You can have the best plan and the latest and greatest technologies, but in the end, it all comes down to the human element."*

A get-started checklist. Protecting your data and information technology systems may require specialized expertise. Depending on the particular industry and the size and scope of the business, cyber security can be very complicated. However, even the smallest business can be better prepared. Here are a few, simple steps to get started:

- **Use anti-virus software and keep it up-to-date.** Activate the software's auto-update feature to ensure your cyber-security is always up-to-date.
- **Don't open email from unknown sources.** Be suspicious of unexpected emails that include attachments whether they are from a known source or not. When in doubt, delete the file and the attachment, and then empty your computer's deleted items file.
- **Use hard-to-guess passwords.** Passwords should have at least eight characters with a mixture of uppercase and lowercase letters as well as numbers. Change passwords frequently. Do not give your password to anyone.
- **Protect your computer from Internet intruders by using firewalls.** There are two forms of firewalls: software firewalls that run on your personal computer, and hardware firewalls that protect computer networks, or groups of computers. Firewalls keep out unwanted or dangerous traffic while allowing acceptable data to reach your computer.
- **Don't share access to your computers with strangers.** Check your computer operating system to see if it allows others to access your hard-drive. Hard-drive access can open up your computer to infection. Unless you really need the ability to share files, your best bet is to do away with it.
- **Back up your computer data.** Many computer users have either already experienced the pain of losing valuable computer data or will experience it at some point in the future. Back up your data regularly and consider keeping a copy of your data off-site.
- **Regularly download security protection updates known as patches.** Patches are released by most major software companies to cover up security holes that may develop in their programs. Regularly download and install the patches yourself or check for automated patching features that do the work for you.
- **Check your security on a regular basis.** When you change your clocks for Daylight Savings Time (DST), evaluate your computer security. The programs and operating system on your computer have security settings that you can adjust. Do you have multiple door locks and a high-tech security system at your office? It could be that tighter security for your computer system is also what you need.
- **Make sure all employees know what to do if the computer system becomes infected.** Train employees on how to update virus protection software, how to download security patches from software vendors, and how to create a proper password. Also, designate a person to contact for more information, if there is a problem.

"I really don't think you can overestimate the value of employee education and awareness when it comes to cyber security," said Chval. "You can have the best plan and the latest and greatest technologies, but in the end, it all comes down to the human element."

"I want to conclude by stressing that sticking your head in the sand, or minimizing the risks from lax cyber security, is done at great peril to organizations and careers," said Chval. "We still commonly see the tremendous fall-out from lax cyber security practices when our clients come to us to investigate or mitigate a cyber incident. This is across a wide range of business types in terms of industries, sizes, and financial wherewithal. And, nine times out of 10, they could have been prevented or mitigated had just a few ounces of prevention been applied." ■

PERFORMANCE

continued from page 27

of appearances or implemented in half-hearted fashion, courts and juries tend to see right through the subterfuge.

What can we learn from court cases?

Avoid vague mandates. In *Brock-Chapman v National Care Network, LLC* (2013), a sales executive filed Family and Medical Leave Act (FMLA) claims after she was placed on a PIP and then discharged within a month of returning from leave to care for her cancer-stricken (now deceased) husband. Under the PIP, which was implemented because of her purported "lack of urgency" for her work, the employee was required to make "significant improvement" within 30 days. Unsure how to meet this vague mandate, she asked for more specific performance goals, but her request was denied. In fact, when forwarding one such request to the employee's supervisor, the HR director referred to the employee as "exhausting," evidencing a discriminatory attitude, the court noted.

By objective measures, the employee was performing quite well — she was 43 percent ahead of her sales target for the year. But the PIP required her to "improve sales." The employee was supposed to have regular calls with her supervisor to monitor her progress toward meeting the PIP goals, but her boss skipped five of the eight calls and did not reschedule them. Moreover, while employees were usually given 90 days to meet PIP objectives, the employee was granted only 30 days. Under these facts, a federal court in Texas let stand a jury verdict in the employee's favor, noting that the questionable intent and execution of the PIP demonstrated pretext.

Employee must have fair chance to comply with PIP. In *Trickey v Kaman Indus Tech Corp* (2012), a federal trial court in Missouri found sufficient evidence that an employer actively thwarted a branch manager's attempts to comply with a PIP. While on the PIP, his superior undermined his eff orts to reestablish his authority as branch manager by publicly congratulating another employee — who was being groomed for the branch manager position — for the branch's excellent performance. An HR manager testified that the PIP process had been manipulated by a supervisor who had asked her to create a PIP for the branch manager when it was inappropriate to do so. A coworker testified that considerable attention was paid to finding the branch manager's mistakes.

When the branch manager asked for additional customer accounts in an effort to meet the sales goals set forth in his PIP, his boss refused the request. Only 58 days into the 90-day PIP, the branch manager was demoted and given a gross sales target of $1.2 million. However, he was assigned customer accounts that had netted only $200,000 in combined sales during the previous year. A jury found the branch manager had deliberately been set up to fail by a sales requirement that was practically impossible, and the trial court upheld the jury's verdict in his favor on his age bias and retaliation claims.

In *Burnsed v Pasco Regional Medical Center* (2012), a hospital placed a respiratory therapist on a PIP. Then the employer removed her from the schedule. Despite the employee's frequent calls to her supervisor and the director of nursing, she was not given any shifts. Ultimately, the employee was terminated, allegedly because she failed to fulfill the conditions of her PIP. The evidence indicated that the employer interfered with the employee's attempts to work enough shifts to satisfy the requirements set forth in the PIP. Thus, a reasonable jury could find that the hospital issued the PIP, removed her from the schedule, and ultimately terminated her because it did not want to deal with her intermittent FMLA absences for asthma and colitis, a federal trial court in Florida held.

The right way to PIP

A bona fide PIP is a good-faith effort to help an employee correct performance deficiencies. To that end, an employer seeks to remove impediments, rather than put obstacles in the employee's way:

- A PIP is implemented in conjunction with HR to control for any unfair bias on the supervisor's part in assessing whether the employee has met stated goals.
- Stated goals are SMART — specific, measurable, attainable, relevant, and timely. Meaningful criteria are provided in order for an employee to gauge progress.
- The employee is given regular feedback. Weekly or semi-weekly meetings with the supervisor are built into the PIP schedule so that more formal feedback can be provided.
- Additional training, mentoring, and "scaffolding" are given as needed or requested.
- A fair amount of time is allowed in which to meet the stated criteria. If a standard PIP is 90 days, then an employee is given the full 90 days in which to meet PIP goals. If business needs require a reduced time frame, the PIP states at the outset the specific time to be allotted, and why.
- Employees are given a sufficient number of shifts or meaningful work assignments during the PIP period in which to demonstrate improvement and satisfy the PIP criteria.
- The consequences of failure to meet PIP goals — usually termination, perhaps demotion — are clearly articulated at the outset.

continued on page 31

RECORDKEEPING

Nine tips for establishing a paperless HR department

Despite cost and environmental reasons to reduce paper use, the completely paperless office has yet to arrive. According to research firm IDC, U.S. companies printed 1.5 trillion pages as recently as 2007. So what's the hold-up? More often than not the answer is the law.

The primary obstacle to going paperless is determining the permissibility of storing legally required documents electronically. In this regard the law has not kept up with the digital age. There is no comprehensive federal or state law governing electronic records retention and management making a totally paperless office virtually impossible.

However, there is some good news. Federal and state agencies are increasingly permitting electronic record retention. For example, the Department of Homeland Security allows employers to fill out and store I-9 forms electronically and the EEOC has approved of electronic recordkeeping for Title VII, ADA, and ADEA documents.

So what is an employer who wants go paperless to do? ERISA regulations in particular provide useful guidance for setting up an electronic recordkeeping system, even for employers not covered by the law. Grace Y. Horoupian and Matthew C. Sgnilek, attorneys at Fisher & Phillips, LLP, gleaned the following tips from those regulations and believe they will help in developing a paperless office and managing electronic records.

1. Make sure your electronic recordkeeping system has reasonable controls to ensure the integrity, accuracy, authenticity, and reliability of the records.
2. Maintain your electronic records in reasonable order and in a safe and accessible place, so that they may be readily inspected or examined, if necessary.
3. Make sure that electronic records can be readily converted into legible and readable paper copy.
4. Electronic records also should have a high degree of legibility and readability when displayed on a video display terminal or other method of electronic transmission.
5. Establish and implement records management practices. Such practices should include: following procedures for labeling of electronically maintained or retained records; providing a secure storage environment; observing a quality assurance program that incorporates regular evaluations of the electronic recordkeeping system including periodic checks of electronically maintained records; and retaining paper copies of records that cannot be clearly, accurately, or completely transferred to an electronic recordkeeping system.
6. Adhere to records management best practices by maintaining the confidentiality of medical records and other sensitive information.
7. Generally, original paper records may be disposed of any time after they are transferred to an electronic recordkeeping system, except that original records should not be discarded if the electronic record would not constitute a duplicate or substitute record as required by state or federal law.
8. Have a system in place that allows you to follow record retention guidelines. This means destroying records in a timely manner. And, don't forget, if litigation is pending or you are aware that litigation is likely, do not destroy relevant documents — even if they are scheduled for disposal.
9. Make sure that your electronic retention and destruction system complies with the most current federal and state law.

There are a number of issues to consider and address in preparing to go "paperless." Although the above guidelines set forth good strategies for converting to a paperless HR record system, employers should contact legal counsel for specific guidance and assistance. ■

PERFORMANCE

continued from page 30

When to PIP

A PIP should be imposed for objective, clearly documented reasons. The decision to place an employee on a PIP must be consistent with his or her recent performance evaluations and merit pay decisions. A PIP must not be imposed in retaliation for filing a complaint or out of a discriminatory belief that an older employee "can't hack it" anymore. An employee should not be placed on a PIP if similarly situated younger workers (or male workers, or white workers, for example) would not have been placed on a PIP based on the performance at issue.

Know when *not* to PIP. A PIP works best to correct performance deficiencies rather than significant misconduct or behavioral issues. In one instance, an assistant principal was placed on a PIP after she strip-searched an 8-year old male student without calling his parents. However, a PIP is hardly appropriate for situations like these, which call for more severe disciplinary measures. ■

Source: *"PIP like you mean it," originally published in the March 1, 2013, Fair Employment Practices Guidelines, a Wolters Kluwer Law & Business publication.*

NLRB

Experts discuss what to expect from the NLRB this year

Perhaps the biggest question looming over the labor environment as we take in the view for 2013 is whether President Obama's recess appointments to the NLRB were constitutional. This question will likely be resolved by the Supreme Court, as the Obama administration has signaled its intent to seek High Court review of the issue. Meanwhile, the Board's "quickie election" rules and every other action of the Board is in limbo, according to Chris Bourgeacq, AT&T General Attorney, Labor/HR for the former Southwestern Bell region, and member of the Employment Law Daily Advisory Board.

In May 2012, the District of Columbia federal district court held the NLRB lacked a quorum when it published a rule revising the agency's representation election procedures (*Chamber of Commerce v NLRB*). In August 2012, the Board filed an appeal of that decision to the D.C. Circuit, and it had been scheduled for oral argument in early April.

In the meantime, in a separate case, the D.C. Circuit concluded in January that the recess appointments were improper (*Noel Canning v NLRB*). In an order issued last month, the D.C. Circuit removed the appeal of the district court's ruling on election procedures from the argument calendar pending further order of the court.

Loss of quorum critical. Similarly, the biggest fight of 2013 may be the president's ability to get new Board members approved by the Senate, suggested Charles Craver, Freda H. Alverson Professor, George Washington University Law School and Wolters Kluwer Labor and Employment Editorial Advisory Board Member. Indeed, Obama has renominated current NLRB members Sharon Block and Richard Griffin, a defiant response to the D.C. Circuit's decision that their recess appointments were unconstitutional.

Beyond the recess appointment problem, 60 votes may be required to get anyone confirmed, which could present a problem, Craver said. If the number of Board members falls below three, the lack of a quorum would be critical. "The absence of a true quorum could invalidate all of the decisions issued," Craver observed.

Union access to employer property. Beyond the questions raised by the recess appointments and quorum issues, what else can employers expect in 2013? Bourgeacq pointed to the Board's decision in *Sodexo America, LLC*, where the board "continued its trend of diluting employers' right to limit access to their property." There, he explained, the Board found that a hospital's policy governing employees' off-duty access to its facility was overly broad when the policy had an exception for employees conducting hospital-related business. "As a result, an employer will need to bar all off-duty employees from access to its property with essentially no exception, or else risk having to allow union organizers onto their property," according to Bourgeacq.

Union use of employer email. Bourgeacq also predicted that the current Board's position will "evolve" with regard to union access to employer email. He noted that in its *Register Guard* decision, the NLRB held unions have no statutory right to access employers' email networks. Bourgeacq thinks we may see "confiscatory" decisions in the future that would open up employers' email networks to unions, unless employers have access policies similar to those in the *Tri-County* cases. In *Tri-County Medical Center*, the Board held that a rule restricting off-duty employee access is valid only if it limits access solely with respect to the interior of an employer's premises, is clearly disseminated to all workers, and applies equally to off-duty employees who want access to the premises for any purpose and not just to those employees trying to access the premises for purposes of union activity.

"Consistent with the Board's increased interest in employees' use of social media, nothing would benefit unions more than unfettered, or at least greater access, to employers' email networks," Bourgeacq pointed out. "Such access would grant union organizers virtual access to the same employees they previously would try to organize face-to-face, without the restrictions that currently exist accessing buildings or other property."

Agency in flux. Turning to the question of whether there will be any changes in the Board's operational strategies or procedures, Bourgeacq observed that the acting general counsel recently consolidated several regional offices, with perhaps more consolidations around the corner. "These actions have altered the leadership, and perhaps bias, of some regions, which in turn could impact the day-to-day operations and decisions reached by the career employees in those offices." Although some former regions may now tilt more toward the employer or the union, it's too early to tell.

"The NLRB is still an agency in search of a newer, broader mission for the 2000s," according to Bourgeacq. "Despite its efforts in the past few years to buoy a sinking unionized workforce, the definite direction of the American workplace is away from unions." He pointed to Wisconsin, Indiana, and Michigan, where unions have suffered serious setbacks. The social media cases represent one way to breathe new life into an agency looking for a makeover, he suggested. "The board's out-

continued on page 33

NLRB

A look at one of the first post-*Noel Canning* suits filed

In one of the first of what may be an onslaught of litigation arising out of the D.C. Circuit's *Noel Canning v NLRB* decision, an employer filed suit against the NLRB for declaratory and injunctive relief, asserting that the Board lacked the quorum required to act. In *Noel Canning*, the court found unconstitutional President Obama's recess appointments to the NLRB.

In January, 2013, District 1199J of the National Union of Hospital and Health Care Employees, AFSCME, AFL-CIO filed a petition with the NLRB seeking certification as the exclusive bargaining representative of patient service technicians and patient center site coordinators working for the employer. The employer objected to the petition on a number of grounds, including that the NLRB and its delegees lacked the authority to order an election or certify the results of an election. Thereafter, a hearing was held before an NLRB hearing officer and in February 2013, the regional director issued a decision and direction of election.

Citing *Noel Canning*, the employer filed suit asserting that the NLRB did not have the requisite quorum. The employee alleges in the complaint that although the Board must maintain a quorum consisting of at least three legitimately appointed members, at the time of the decision, there was only one such member. Although Chairman Mark G. Pearce was appointed by President Obama and confirmed by the Senate, Sharon Block and Richard Griffin were allegedly appointed pursuant to the Recess Appointment Clause of the Constitution. The latter two appointments were not confirmed by the Senate. In *Noel Canning*, the D.C. Circuit held that the appointments of Block and Griffin were invalid because they did not occur during a recess and thus were unconstitutional.

Additionally, the employer asserted that when the Board is unable to act, delegations to regional directors are inoperative. Moreover, although regional director decisions could typically be appealed to the Board, in this instance, the Board had no authority to act because it lacked a quorum.

Although the employer filed a motion to dismiss on these bases before the regional director, the regional director denied that motion, indicating that he strongly disagreed with the D.C. Circuit's reasoning that the Board lacked a quorum. Instead, he concluded that the Board could and should continue to perform its functions, and ordered the employer to provide a list of eligible voters.

The employer argued that the regional director did not have authority to order the election and that his actions in doing so would cause immediate and irreparable injury to the employer. For example, the election process would require the disclosure of a sensitive "Excelsior list" of employees' full names and home addresses to the union, and this itself created irreparable harm, the employer asserted. Though the current Board had no authority to compel disclosure, once disclosure was made, it could not be reversed.

Moreover, the employer alleged that the Board could not certify an election result and that, therefore, the employer and union would "exist in that state of post-election, pre-certification limbo for an indeterminate period of time, during which [the employer] will be significantly constrained from altering the terms and conditions of employment of any employee or group of employees in the proposed bargaining unit."

Accordingly, the complaint requests that the court declare that the NLRB and its regional director are without statutory authority to enforce the February 2013 order or to require, conduct, or certify a union election on behalf of the specific employees. It also asks that the court enjoin the NLRB from enforcing "its invalid February 26, 2013 order" and from requiring, conducing, or certifying an election on behalf of those workers until it has authority to do so. ■

NLRB

continued from page 32

reach efforts, such as revising its website to highlight its actions against nonunion employers, are another way for this agency to reestablish relevancy under a perhaps outdated labor law."

Agency funding. What about the impact of funding on the NLRB's activities in 2013? Craver assumes there will be reductions in funding that will result in loss of some of the Board's staff. "This may make it difficult for the Board to hold elections as quickly as it would like and to resolve unfair labor practice cases as quickly. On the other hand, the reduction in the number of representation elections being conducted should minimize the impact of this factor." The Board is also not seeing as many truly significant unfair labor practice cases, which should also make it easy for the Board to continue to function effectively—if it can continue to have at least three members, Craver suggested. ■

Source: *Written by Pamela Wolf, J.D. "Looking back and ahead: NLRB—the year ahead," was taken from the March 15, 2013, issue of Employment Law Daily (www.employmentlawdaily.com), a Wolters Kluwer Law & Business publication.*

HR Notebook

Sharp rise in gasoline prices causes increase in February CPI

The Consumer Price Index for All Urban Consumers (CPI-U) increased 0.7 percent in February on a seasonally adjusted basis, the U.S. Bureau of Labor Statistics (BLS) reported March 15. Over the last 12 months, the all items index increased 2.0 percent before seasonal adjustment.

The gasoline index rose 9.1 percent in February to account for almost three-fourths of the seasonally adjusted all items increase. The index for all items less food and energy increased 0.2 percent in February. The indexes for shelter, used cars and trucks, recreation, and medical care all rose in February. These increases more than offset declines in the indexes for new vehicles, apparel, airline fares, and tobacco.

The all items index increased 2.0 percent over the last 12 months compared to a 1.6 percent increase for the 12 months ending January. The index for all items less food and energy also increased 2.0 percent over the last 12 months. The energy index increased 2.3 percent and the food index rose 1.6 percent.

Real average hourly earnings fall 0.6 percent in February

Real average hourly earnings for all employees fell 0.6 percent from January to February, seasonally adjusted, the BLS reported March 15. This result stems from a 0.2 percent increase in average hourly earnings being more than offset by a 0.7 percent increase in the Consumer Price Index for All Urban Consumers (CPI-U).

Real average hourly earnings rose 0.1 percent, seasonally adjusted, from February 2012 to February 2013. The increase in real average hourly earnings, combined with a 0.3 percent decrease in the average workweek, resulted in a 0.2 percent decrease in real average weekly earnings over this period.

Payroll employment up in February as unemployment edges down

Total nonfarm payroll employment increased by 236,000 in February, and the unemployment rate edged down to 7.7 percent, the BLS reported March 8. The unemployment rate has shown little movement, on net, since September 2012. Employment increased in professional and business services, construction, and health care. The number of unemployed persons, at 12.0 million, also edged lower in February. In the prior 3 months, employment had risen by an average of 195,000 per month.

Professional and business services added 73,000 jobs in February; employment in construction increased by 48,000; health care employment increased by 32,000; employment in the information industry increased by 20,000; and retail trade added 24,000 jobs.

IMMIGRATION

USCIS issues revised Form I-9

The U.S. Citizenship and Immigration Services (USCIS) on March 8 issued in the *Federal Register* a revised Employment Eligibility Verification form, Form I-9. Revisions include formatting changes and the inclusion of additional data fields, the agency reports. Employers are required to use the Form I-9 to verify the identity and employment authorization eligibility of their employees.

The modifications include an expansion of the Form I-9 from one to two pages (not including the "List of Acceptable Documents" and form instructions), additional data fields (such as the new hire's email address and phone number), enhanced Form I-9 instructions, and a revised layout.

The new form took effect immediately upon publication in the Federal Register and will become the only acceptable version of the form as of May 7, 2013. Until then, the USCIS has provided a 60-day grace period during which the current version of Form I-9 will remain valid for use. Therefore, during this 60-day grace period, employers may continue to use the February 2, 2009 and August 7, 2009 versions of the Form I-9.

Employers do not need to complete the new Form I-9 for current employees for whom there is already a properly completed Form I-9 on file, unless re-verification applies.

Additional information can be found at the USCIS website: www.uscis.gov/i-9central. ■