nase®

SelfInformed

Published by the National Association for the Self-Employed

May 2016

TABLE OF CONTENTS

NASE Member
Wendy Miller

CYBER SECURITY & DATA HACKING

Here we provide some guidelines and specific tips on what businesses can do to help protect their own and their customer's data. We explain what some of the dangers on the internet are, dispel some misconceptions about password management, stress that two-factor authentication is absolutely essential for security, emphasize that you need a forensics partner, and explain what banks are doing or not doing to help keep credit cards safe.

THE DANGER OF THE INTERNET

Over the past few decades, the internet has definitely shoved business far ahead in productivity. It has opened new markets, created new businesses, and let businesses interact with their customers more effectively. But the internet is a dangerous and hostile terrain today as criminals have flocked there too. Given that hazard, you and your business need to learn about the risks of working online to protect your customers and yourself.

Small businesses and entrepreneurs of all sizes have a responsibility to keep data safe. In some cases it is the law, like HIPAA and SOX. Everywhere else it is just necessary if one does not want to suffer litigation or other damage to their business or customers' business. It does not matter whether the business has 10 customers or 10,000. It does not matter whether a company sells high-tech products or low-tech ones nor does it matter if that business has 1 technical support person or 100. In all of these situations companies process data via computers, most of which are connected to the internet. There is inherent risk in that because of cybercrime.

Even the largest, most technically adept businesses get hacked. So does the military and government. That means there is nothing that is hacker proof. So if a vendor tells you that they can guarantee that they will protect your data 100% of the time, go find another vendor.

DEFENSE IS THE BEST OFFENSE

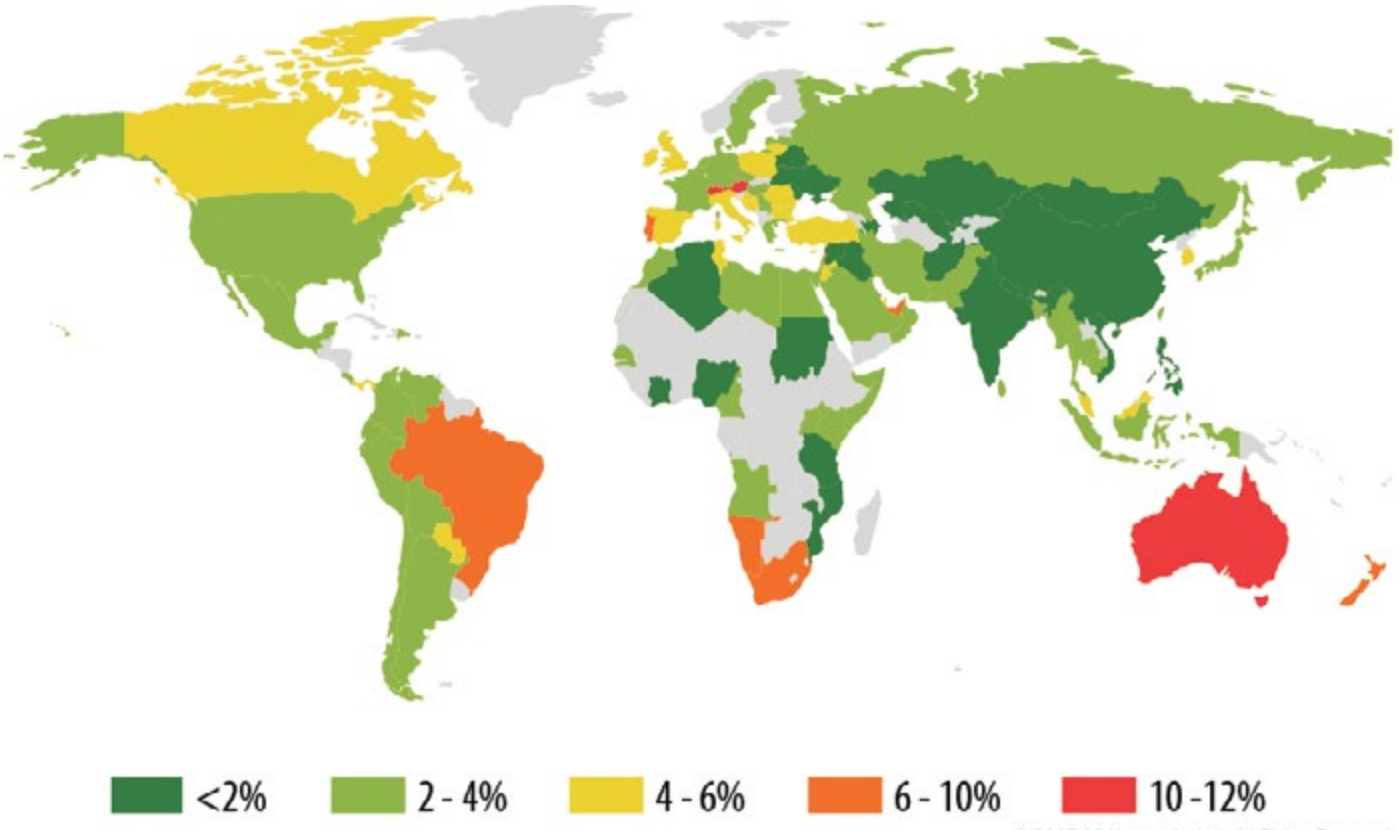
There is really no difference between being hacked and having viruses on your computer. The former term sounds more serious. But they are the same. This is because hackers use viruses to steal data. A computer virus can be a small annoyance that causes pop up ads or it can be something more complex designed to turn your computer into a robot to attack other computers. Or it can steal an entire database, record customer transactions at a checkout terminal, or record keystrokes.

Given that definition, the best way to approach cybersecurity is to assume that you already have been attacked. (**Statistics say** you probably already have been attacked and don't know it. The graphic below shows that from 33-43% of computers in the USA have a virus right now.). The only question is to what degree you have been hacked, meaning what kind of attack are you suffering.

The defensive posture prepares you to react in a calm and controlled manner when a really large attack occurs. Then you won't do what SONY did when it was attacked by North Korean hackers. They simply unplugged everything, shut down the business, and called for help. They were completely caught off guard, so that is what they did.

Working from the defensive posture, you realize a few things right up front:

- Businesses need a forensics partner on standby to help them when they get hacked. This is a security firm that steps in to help you figure out how much data has been stolen, eliminate the current threat, shore up your defenses, and help with some fundamental problems like employee security awareness training.
- You need a communication plan to inform your customers when their data has been stolen. This can be the most difficult of your problems.



Graphic Source: Kaspersky

- We will repeat this one again: it is crucial to train employees in security awareness. Employees are the **number one weakness in security** because they do not pay attention to what they click on. Hackers prey on human weakness to trick people into doing that. They downloads viruses, which go right around any defenses. Firewalls and such do not work when the person who downloads a virus is inside your company: those things work from the outside in.

- You need to classify data as to its importance and assess what private company or customer data you are keeping where. For example, credit and debit card numbers and their pin should never be stored in the same database. Do not put financial data that you do not need into every system.

Whether you are a 100 year old family business or a growing new business it is necessary to adapt to the shifting technological landscape. All of those iPads, iPhones, and other fancy gadgets let your employees take their sales to your customer's office. But those devices also provide criminals with new platforms from which to attack your data.

Do not panic. Self-employed people do not need a costly army of technical people to contain these risks. All the expertise they need is in the cloud, where they can rent it and do not have to hire it. In other words, it is not necessary to pay a company to come to your office to set up a secure ecommerce system so that you can sell your products from the web. All a small business needs to do is sign up with a cloud company like Stripe who provides that or use the ecommerce ability of hosting companies like Rackspace. There is less risk in using the cloud because there is nothing to install in your office or customer site. By definition every time you install software it exposes new security weaknesses. So avoid that. Use the cloud because it only requires a web browser. True, that is subject to attack too, but Google, Apple, and Android automatically patch their browsers against the latest security weakness. So there is some lag time during which you are vulnerable: this is the time between when hackers find the weakness and the software companies fix it. That can be days, months, or years.

CYBER MISCONCEPTIONS: PASSWORDS

People often behave, as the saying goes, like sheep: they will follow each other right over the cliff because they do not question whether what they habitually do is logical. A good example of that is password maintenance. It is **absolutely true** that a longer password is better than a short one. But it is **not true** that one with lots of strange and hard to remember characters is better than simple words. The former is often even less secure.

Consider, for example, this example. Which password is hard for a hacker to crack?

LL##$$llll121

Or

butter.knife

There are several problems with the first one. First, it is too hard for a person remember. So people are going to do what you would expect in that case and type that into a document. Then they copy and paste it when they need it. So it's right there for a hacker to steal. The second password is sufficiently long, yet easy to remember. So there is no need to write that down. You can even make using regular words in passwords a company rule. So don't listen to the consultants who insist that you adopt a complicated password scheme. The most important thing is password length as longer passwords take more computer time (sometimes years) for a hacker to attack. And require people to keep their business and personal passwords different. You would not want a hacker to use

passwords they have stolen from, say, a dating website, to login to your inventory control system.

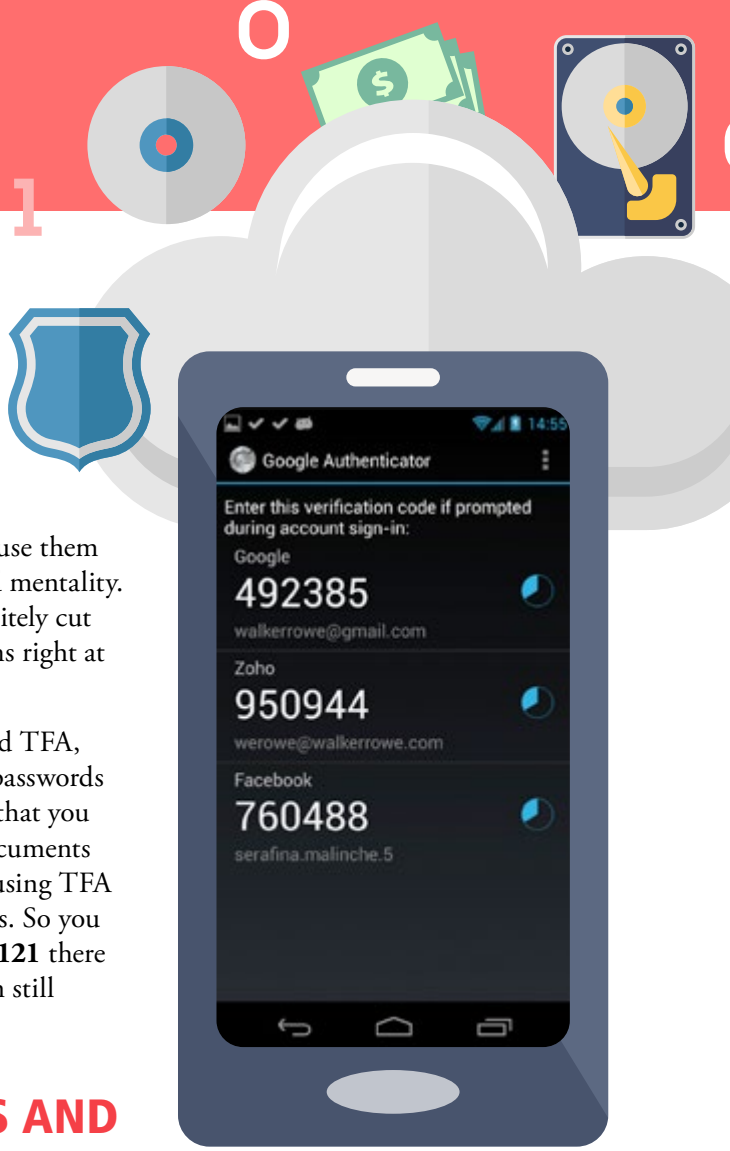
TWO FACTOR AUTHENTICATION: THE ONLY SAFE PASSWORD IS NO PASSWORD

You should not use any system that requires only a password and nothing else. Instead you should only use systems that support two-factor authentication (TFA). TFA works by sending a code to your cell phone or email that you have to type into the screen in order to log in. A hacker can steal your password by installing a virus on your computer that records your keystrokes or just steals the user database. But they are not likely to have stolen your phone as well as your password.

Some common websites and applications that support TFA include Wells Fargo CEO Portal, Gmail, Outlook.com, Office 365, Dropbox, Google Apps, Facebook, E*Trade, SalesForce, and others. If your vendor does not support TFA then pick another vendor. Or if there is no other choice then you can put **Okta** in front of that.

The TFA code generated by the application must match the code that is generated with a cellphone app, like the Google Authenticator, shown below. The computer generates this code using the current time and a randomly-selected number that is unique to the user. So the time on your cellphone needs to be somewhat close to the correct time. But a few minutes error either way is OK.

So if you think through this a little bit, and do not behave as a sheep, you will realize that if you need a code to log in to an application then you do not a password at all. Yet, as we said, most apps still use them because people have a herd mentality. Either way, TFA will definitely cut off lots of hacking problems right at the source.



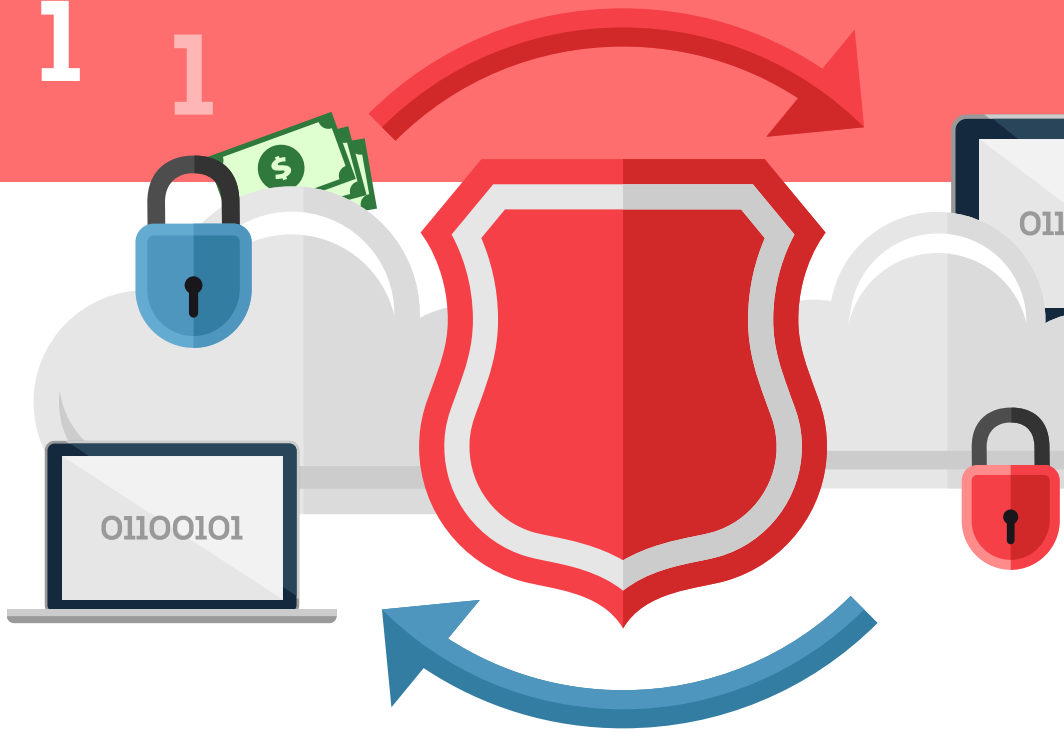
Now that you have adopted TFA, there is no risk in storing passwords for the many applications that you use in Google or Word documents online, as long as you are using TFA to protect those documents. So you can even copy **LL##$$llll121** there if one stubborn application still requires that.

CREDIT CARDS AND CYBER CRIME

Hackers offer **stolen credit cards for sale** on the internet for as little as a few dollars. These criminal rings have grown so large and sophisticated that they even guarantee their customers that the stolen card will support a certain number of charges before the fraud department or credit limit shuts it down.

The truth is that banks in the USA are not doing the best possible job of protecting customers against this kind of theft. They have thrown out common sense and instead adopted the desires of the marketing department who argue for simplicity over security. Banks and the leading credit card companies do not want to lose market sharing to emerging payment systems, like digital wallets, and online payment firms, like PayPal. So they do not always do

Banks and the leading credit card companies do not want to lose market sharing to emerging payment systems, like digital wallets, and online payment firms... so they do not always do what is most prudent.



what is most prudent, like requiring a pin. Some require only a signature, which, of course, can be faked.

Yet, there has been change. **EMV cards** have a small computer chip to encrypt the card data. Yet the problem with using an EMV or other advanced card is it does not work on your web site, as there is no one there to physically present the card to the POS (point of sale) terminal.

The best thing to do then is, as we said above, use a cloud vendor like PayPal or Swipe, who should have the best security. And for in-store transactions, work with your POS device vendor to make sure those are secure. Those devices are subject to hacking just like any other computer. That is where hackers **stole** more than 100 million credit and debit card numbers from Target.

EDUCATION IS THE BEST POLICY

In summation, the best approach to security remains educating yourself and your employees about the risks inherent in the internet and how to be safe. That means training new employees and retraining existing ones. Many websites offers training in this area. Then find a forensics security partner. They call themselves Managed Security Services, but you can sign up for less than their full offering. Also use TFA instead of passwords. Adopt cloud payment systems, and use the cloud for most other applications as well, instead of installing your software. And do not fall for any security firm or product who offers 100% protection. Go with someone who is honest about the risk. And if you are large enough to have people to do that, write a risk assessment for your business to help identify where you are most exposed and to develop a communication plan.

The best approach to security remains educating yourself and your employees about the risks.

Ask the Expert

Q: *How long should I keep my tax records and what is the best way to secure them?*

A: We have all heard about the paperless society that the world is moving toward, but unfortunately the IRS is not yet on board with that process. Your tax return still today can be best supported with a stack of paper. How long to keep that stack of paper can be confusing. The IRS can examine your tax returns for up to three years from the date you actually file the return. So if you file your 2015 federal income tax return on April 15th of 2016, the IRS can choose to examine that return at any time through April of 2019. However, if you filed an extension and ultimately file your return on October 15th, then the IRS will have until October 15th of 2019 to ask questions about your 2015 tax return.

From a technical standpoint, you should keep your tax records and related support for three years, but if you can keep those records for four years, then you will never need to remember if you filed on April 15th or October 15th. Therefore, tax records for 2015 should be retained through 2019, and 2016 records should be maintained through 2020 and so on.

It is certainly a good idea to convert the actual paper into some electronic form of filing system, but not required. If you can scan your personal stack of paper and save a digital copy of the records in addition to the actual paper, you may very well avoid the angst of water damage or other destruction of the paper and might also enable actually locating the detail two years from now when the IRS does decide to send you that letter asking for more information. As always, and for many reasons, it is also a great idea to make sure you have committed to maintaining a separate bank account for your business. By making sure all of your activity related to the business runs through that dedicated business bank account, your bank will now also have a digital copy of a vast majority of all of your support. Even if your system of retention fails, your bank will still maintain the detail of your transactions. So if you haven't done it yet, go down to your bank on open that separate bank account. If something happens to your records, you will be glad you did.

As always, don't forget that you are not alone. Bookmark our website at **NASE.org** as well as the IRS website at **IRS.gov** you will always be able to find the help you need.

New!

Member Benefits

Visit www.NASE.org to learn more about the following benefits!

Unfortunately, identity theft is a real threat every day. So don't wait until you become another statistic, start protecting your vital personal information today. It takes just minutes to sign up-and then you can rest easy. But don't take our word for it, try LifeLock® protection today and get it FREE for 30 days plus 10% OFF*

ENROLL TODAY!

LifeLock® Standard™

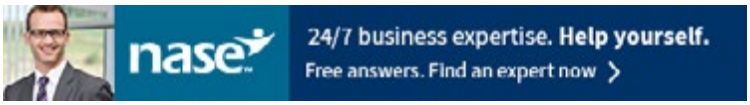
LifeLock® Standard™ identity theft protection uses innovative monitoring technology and alert tools to help proactively safeguard your credit and finances.

LifeLock® Advantage™

LifeLock® Advantage™ service provides enhanced identity theft protection, including important notifications beyond financial and credit fraud.

LifeLock® Ultimate Plus™

LifeLock® Ultimate Plus™ service provides peace of mind knowing you have the most comprehensive identity theft protection available. Enhanced services include bank account application and takeover alerts, online credit reports and credit scores.



Information Technology Experts

Our experts have an extensive background in building and maintaining small business applications of all types relating to content management systems, search engine optimization and even hardware and other related technologies necessary to support a wide variety of IT solutions. We know what it's like to be frustrated with the many "solutions" out there and NASE is here to help steer you to the right solution for your needs and within your budget.

SaveAround™
Your LOCAL Discount Savings Book.

SaveAround® Welcomes NASE Members! As part of the NASE's preferred membership with SaveAround®, members will receive an annual digital membership with the purchase of any SaveAround® Coupon Book.

Benefits:

- Receive extremely rich discounts from local businesses in their hometowns in a simple turnkey product.
- Access to mobile and digital offers for even more savings nationwide.
- Opportunity to save even more with SaveAround's national partners across the US.
- Provide these great discounts as a gift for your employees, customers, or for your own family.
- Use as a great marketing tool for your small business to attract customers.

Member Spotlight

Self-Employed for Seniors

The NASE and Annapolis Senior Care Solutions would like to thank Atria Manresa, an assisted living facility in Annapolis, MD for allowing us to have the photo shoot at their facility.

Wendy Miller *is the owner and Principal of* ***Annapolis Senior Care Solutions*** *located in Annapolis, Maryland. Additionally, she holds her LCSW-C license and is an approved supervisor through the State of Maryland Board of Social Work Examiners. Annapolis Senior Care Solutions specializes in helping seniors maximize their quality of life. Their goal is to provide seniors and their families counsel about lifestyle choices and services that maximize health and wellbeing. Wendy has been a member since 2014.*

"The emotional attachment to your own business's success can be challenging at times. I overcome this by surrounding myself with supportive friends and colleagues who encourage me as needed."

What inspired you to enter the field you are in?

I have always enjoyed helping people, which is why I pursued an undergraduate degree in Psychology and a Master's degree in Social Work. I began specializing in working with seniors early in my Social Work career through various medical and senior residential settings where I was working. I recently gained my certification as an Aging Care Specialist™, as I wanted to focus more closely on geriatric care management services for seniors and their families.

When and why did you start your business?

I officially launched my own business, Annapolis Senior Care Solutions, a geriatric care management practice, in the fall of 2015. This was a concept I had in mind for many years, as I have always wanted to solely focus my professional expertise on helping seniors and their families make sound decisions about the best way to successfully age.

What challenges have you faced in your business? How have you overcome them?

The emotional attachment to your own business's success can be challenging at times. I overcome this by surrounding myself with supportive friends and colleagues who encourage me as needed.

How do you market your business?

I market Annapolis Senior Care Solutions through social media and several local print newsletters and publications targeted at seniors in my service area. I also regularly network with any and all local providers of senior care including assisted living and nursing facilities, home care companies, elder law attorneys and financial planners.

Do you have any employees?

No, I do not have any other employees; however, plan to add employees as needed as my business grows.

What's your schedule like, what's a typical day for you?

My typical day is usually divided into two parts. The first part involves client visits, phone consultations and clinical follow up as needed. The second part of the day is dedicated to marketing and business operations.

What's the best compliment you've ever received from a client?

I have had many clients tell me that I truly have helped them and/or their family members during a challenging time. This is what I truly care about and it is gratifying when someone shares with me how I helped them.

What's the best thing about being self-employed?

The best thing about being self-employed is that I can focus on the type of work that I feel I best excel at, and I also have the opportunity to learn about various aspects of business development that I had not worked directly in previously.

What's the most important piece of advice you would give to someone starting their own business?

I would advise anyone starting a business to identify colleagues and professionals who can act as mentors during this process. I would also advise to be financially prepared to reinvest early profits back into your business in order to further grow your business.

"The best thing about being self-employed is that I can focus on the type of work that I feel I best excel."

Want to be Featured in Upcoming Issues?

Log onto **NASE.org** and fill out the **Get Publicity** form. Don't miss this unique opportunity to showcase your business and get noticed by your fellow NASE members.

Learn More in the NASE Member Directory

Learn more about other Self-Employed businesses in the **NASE Member Directory.** You can add your own company to the NASE Member Directory at no charge – it is a free benefit to NASE members.

NASE Joins Coalition Ahead of DOL Announcement on NEW OVERTIME REGULATIONS

The NASE has joined the **Partnership to Protect Workplace Opportunity** in advance of the Department of Labor's proposed new overtime regulations, expected to be released before Memorial Day.

On March 13, 2014, President Barack Obama issued a memorandum directing DOL to "modernize" the FLSA overtime regulations governing eligibility for the white collar exemption. On July 6, 2015, DOL published proposed changes to the regulations. The proposed regulation would increase the salary threshold for exempt employees. DOL proposes increasing the current threshold of $455 per week ($23,660 annually) by 113% to $970 per week (or $50,440 per year), which the agency estimates will be the 40th percentile of earnings for all full time salaried workers in 2016.

DOL has submitted the final rule to the Office of Management and Budget (OMB) for final review—this is the final step before the Overtime rule is published. We anticipate the final rule to be released sometime in the early summer.

The Coalition is surveying small businesses to fully understand the impact of the proposed regulations on your business, **please complete the survey here**.

President Barack Obama issued a memorandum directing DOL to "modernize" the FLSA overtime regulations governing eligibility for the white collar exemption.

Katie Vlietstra is NASE's Vice President for Government Relations and Public Affairs; You can contact her at **kvlietstra@nase.org**.