

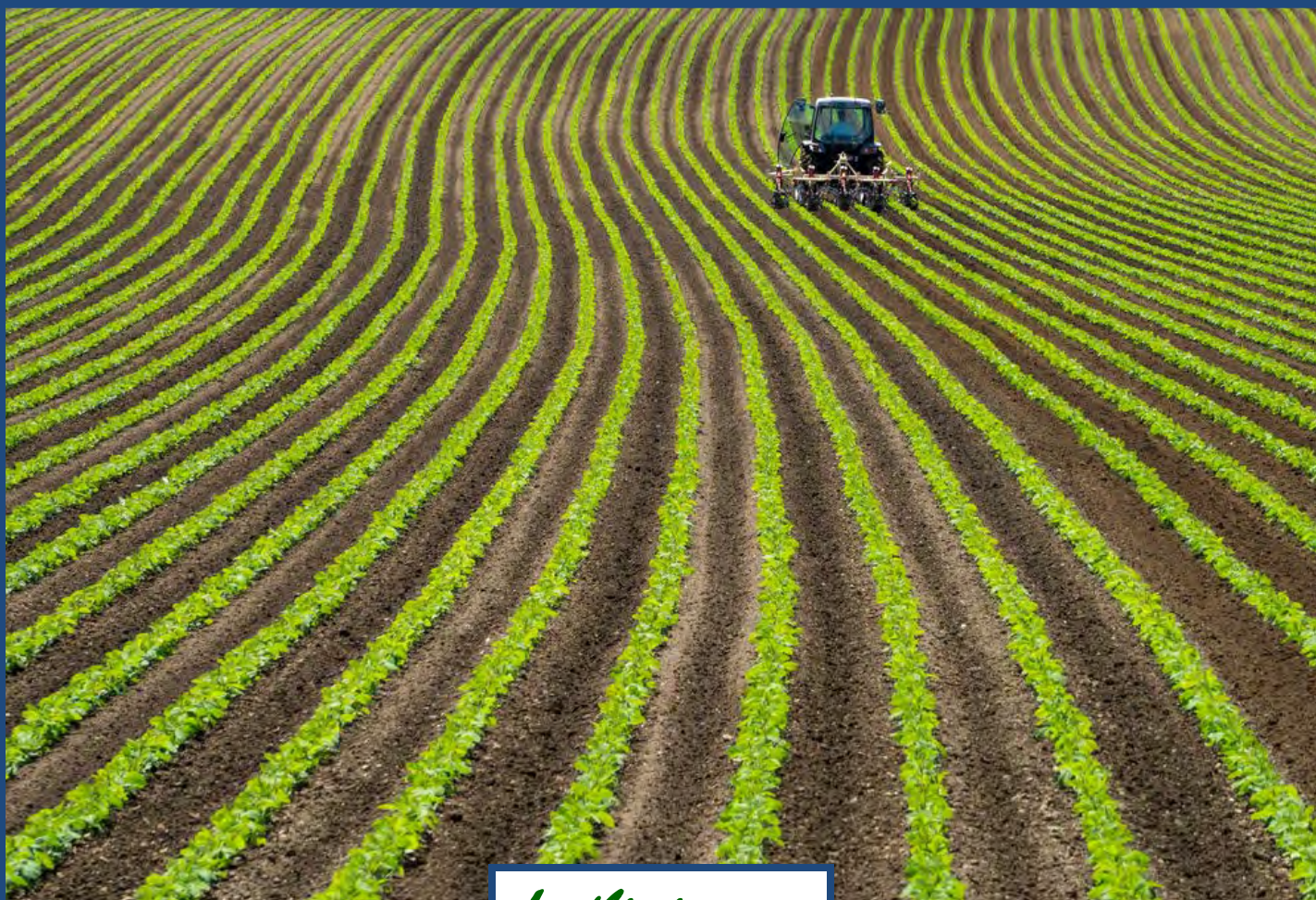


INTELNET *News*

Official Newsletter of the
International Intelligence Network, Ltd.

Intellenetwork.org

Summer 2017



In this issue ...

PETER'S POSTING

By Peter Psarouthakis.....2

MEMBER NEWS.....3

ARUBA BECKONS

By George Michael Newman.....6

PROTECTING HUMAN ASSETS

By Neal Custer.....7

TRUTH, HONOR AND PROMISES

By Weeden Nichols.....10

ISPLA REPORT *by Bruce Hulme*..... 11

PROTECTING YOUR BUSINESS: ARE YOU PREPARED?

AN INTELNET AND FINLEY CONSULTING WORKSHOP

.....18

Copyright 2017, International Intelligence Network. All rights reserved. Articles are on the authority of the author. Nothing herein should be construed as legal advice without consulting the appropriate legal authority.

Peter's Posting

by

Peter Psarouthakis
Executive Director, Intellenet



Dear Intellenet Members:

Our 2018 conference hotel registration web site is up and running, and ...

We are now half way thru the summer and I hope that you all are doing well. Plans are well under way for our 2018 conference in beautiful Aruba from April 10-13 at the beautiful Aruba Marriott Resort & Stellaris Casino, located at L.G. Smith Boulevard # 101, Palm Beach, Aruba. Both the education and conference team is hard at work planning another stellar training and networking event you won't want to miss. I am excited to announce the hotel reservation website is up and running and can be accessed by going to the Conference page of the Intellenet website, special thanks to Peggy Centonze, our Executive Assistant for designing the conference page.

We continue to see members who have not renewed due to retirement, and we wish them well and thank them for their years of support. However, that also means we need to recruit new members. As you go about your business and meet investigators in your travels, please be aware of any potential candidates for membership. Remember that they must have at least ten years of investigation experience.

We continue to offer educational opportunities to not only our members but outside professionals. Intellenet and Finley Consulting & Investigations are pleased to offer a two-day workshop, September 14-15, 2017, at the Pittsburgh Marriott North Hotel in Cranberry Township, PA. Attendees will earn 14 CEUs and network with other safety and

security personnel. This two-day intensive workshop will demonstrate cost-effective measures to reduce your potential for death injury and increase your reputation with your customers as a safe place to conduct business. There can be no guarantee that a hostile action may occur, but your preventive actions should reduce your exposure to negligence security litigation claims. More info on can be found by clicking on the workshop link on our web-site, again thanks to Peggy!!!



Our Facebook group continues to grow. Approximately 1/5 of our members are on the Facebook group. If you use Facebook please ask to join the group. The group

is for members only and all people are checked against our membership list before being allowed into the group. The Facebook group does have postings with additional information from members that typically are not allowed on our general listserv. The Facebook group link is <https://www.facebook.com/groups/574462629397889/>.

Lastly, Intellenet will be exhibiting at the North Carolina Association of Private Investigators Conference in Cherokee, NC, November 5-7. We will also be exhibiting at the Minnesota Association of Private Investigators Conference at Mystic Lake Casino located in Prior Lake, MN, September 27-29. On behalf of the entire Board of Directors, I hope everyone has a great rest of the summer! As always you can reach me at peter@ewiassociates.com.



Member News

Welcome New Members ...

Uffe BODEHOLT — Copenhagen, DENMARK
Marc BOURNE – Bensalem, PA
Danny BRABHAM—Roanoke, VA
Arnold (Arnie) BRISCOE – Willis, TX
Larry FLANNERY – Greensboro, NC -
- added to Greg Scott listing
Larry FORLETTA – Pittsburgh, PA
George GERGIS — South Bend, IN
Tom HAM – Knoxville, TN
Marc HURWITZ – Miami, FL
Dan LOPER – Boston, MA / Portsmouth, NH
Jeff MUELLER — New York City
Tasha SIMS — Little Rock, AR
Bernarda SKRABAR - Ljubjiana, SLOVENIA
Susan SPOFFORD—Fairfax, VA

These are our new members since we last published. To update your membership listing on the web, or in our Briefcase Roster, send info to intellenet@intellennetwork.org.

In the news ...



Former FBI agents John Mindermann and Paul Magallanes were quoted in a lengthy [New York Times](#) article involving past FBI investigations that have centered on White House activities and U.S. Presidents.

Paul is an Intellenet member. The article focused on how the FBI views itself as an independent and necessary check on the powers of the president. Thanks to [Bruce Hulme](#) for alerting us to this news.

News from the UK ...

Phil and Yin Johnson announced that their founder members status on @ResilienceCloud has been updated to include their new capabilities, including the social /business media information. Their site was created by member [Rodney Johnson](#) of Seoul.



Phil also noted they have a new business address in the UK: Phil and Yin Johnson | J J ASSOCIATES INTERNATIONAL | 506 Thornton Road | Thornton, Bradford BD13 3JD United Kingdom.

News from PI Magazine ...

Roe and Jimmie Mesis have announced that fellow Intellenet member [Jim Nanos](#) and his business partner [Nicole Cusanelli](#) have become the new owners and publishers of [PI Magazine](#).



Jimmie will continue as an Associate Editor to assist in the transition, as PI Magazine continues its proud tradition. Jimmie and Roe will now focus their efforts on their investigative agency and national countermeasures company, [USA Bug Sweeps](#). Congratulations Jim and Nicole, and thank you Roe and Jimmie for building a successful magazine, one of its kind in the professional investigator literary canon.



Continued on next page ...



1625 Prince Street
Alexandria, VA 22314-3
USA
+1.703.519.6200
Fax: +1.703.519.6299
www.asisonline.org

June 6, 2017

Mr. James P. Carino, Jr., CPP
Senior Consultant
Executive Security Consultants
PO Box 350
Gladwyne, PA 19035-0350

Dear Mr. Carino,

This year marks the 40th anniversary of the ASIS Certified Protection Professional program. We will celebrate this milestone at the ASIS 63rd Annual Seminar and Exhibits, September 25-28 in Dallas. Because you are one of only four people who have held the CPP for all 40 years, we would also like to celebrate you at this year's Seminar.

We would be honored for you to be our guest for the Seminar. ASIS will cover the costs of your travel and lodging during the event as well as provide a complimentary full-conference registration. I have asked Gayle Rosnick, ASIS's Certification Director to handle all your travel and Seminar needs. Gayle's email address is gayle.rosnick@asisonline.org and her phone number is 703.518.1412. Please RSVP directly to Gayle and she'll take it from there!

ASIS greatly appreciates your continued dedication to the CPP program. We hope you will allow us to thank you in person for your continued support.

Sincerely,

Thomas J. Langer, CPP
2017 ASIS President

Peter J. O'Neil, CAE
Chief Executive Officer

News from Jim ...

Our esteemed founder and Executive Director Emeritus, **James P. Carino Jr., CPP**, recently received notice that he is the recipient of a special distinction to be bestowed by ASIS International at their annual conference this year. Jim shared the letter he received from ASIS.

Jim had to reply to ASIS that he wouldn't be able to attend this year's conference. At present he and Connie plan to fly to Italy for the annual reunion of the Aviano Air Base Association. In addition: "Grandson number 2 is doing a semester abroad in Florence (he did spring semester in London). He starts his 4th year at the Syracuse School of Architecture (a 5 year program)."

Jim sent us his new address: 3500 W. Chester Pike, CH 110 | Newtown Square, PA 19073 | Ph: 215-680-4296.

Congratulations, Jim !

Member News continues on next page ...

News on the ETS Initiative ...



Dave Ziegler sends us an update on the Intellenet initiative featuring audits for the Educational Testing Service (ETS):

“To date in 2017, our members have conducted ETS files in 63 countries. Since June 30, 2017, one of our members in the Euro Zone conducted 45 test security audits. Our members reached several new countries this year, including the following:

- Burkina Faso
- Djibouti
- Ethiopia
- Kyrgyzstan
- Turkmenistan
- American Samoa (not a country but hard to get to!)

This brings our total countries reached in the last few years to well over 150! In the USA we conducted both investigations and audits in 16 states with over 158 files. I would suggest that all our members can tell prospective clients that we indeed have International reach with proven results.”

Founded in 1947, ETS is “... the world's largest private nonprofit educational testing and assessment organization. It is headquartered in Lawrence Township, New Jersey, but has a Princeton address.

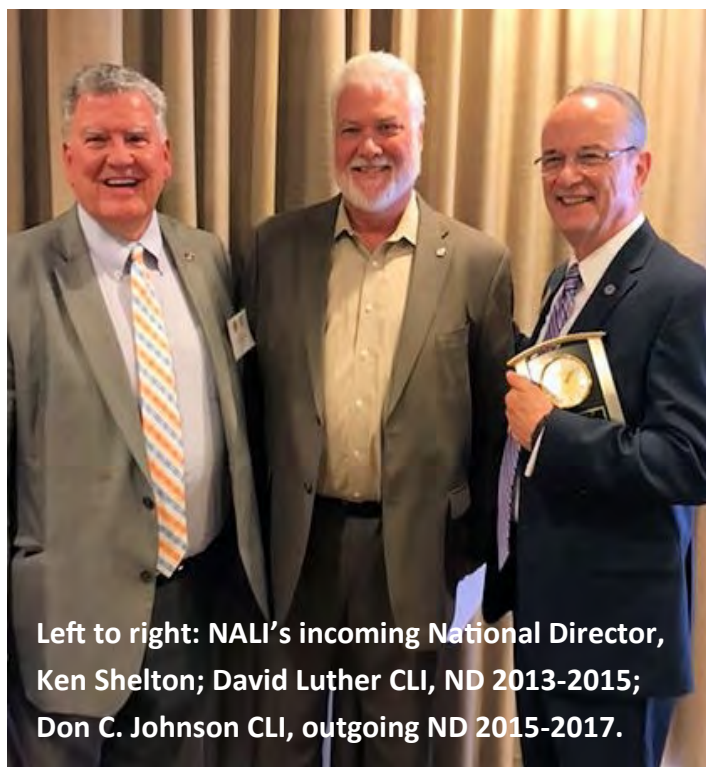
ETS develops various standardized tests primarily in the United States for K–12 and higher education, and it also administers international tests including the TOEFL (Test of English as a Foreign Language), TOEIC (Test of English for International Communication), Graduate Record Ex-

amination (GRE) General and Subject Tests, and The Praxis Test Series — in more than 180 countries, and at over 9,000 locations worldwide ...” (Source: [Wikipedia](#))

For more information on the ETS initiative, contact Dave at cpstaats@verizon.net, phone 609-538-0508.

News from NALI ...

The National Association of Legal Investigators and Intellenet “share” many members and for years Intellenet members have been active in both associations. That tradition continues after [NALI's](#) 50th anniversary conference and celebration, in June in Alexandria, VA, with **Nicole Bocra Gray** as conference chair. NALI had record numbers in attendance, and the celebration featured a dinner cruise on the Potomac River. Several Intellenet members were elected to NALI's Executive Council, which takes office on September 1st, including: **Ken Shelton**, National Director; **Nicole Bocra Gray**, Assistant National Director; Region Directors **Alan E. Goodman**, Region I; **George Gergis CLI**, Region II; **Jay Marin**, Region III; **Dave Johnson**, Region IV; and **Anne La Jeunesse**, Region VII. For several years, Intellenet members have served as NALI's CEO, three of whom are seen here.



Left to right: NALI's incoming National Director, **Ken Shelton**; **David Luther CLI**, ND 2013-2015; **Don C. Johnson CLI**, outgoing ND 2015-2017.

Continued on next page ...

News in private security ...

Intellenet member **Tom Cseh** (*center, in photo*) received the prestigious Outstanding Staff Contribution Award for 2016 at the U.S. Security Associates (USSA) Winner's Circle XII presentation in Phoenix, Arizona on April 22, 2017. Tom is Andrews International's Regional Director for Operations in Latin America, based in San Pedro Sula, Honduras. Presenting the award to Tom was Richard Wyckoff (*right*), President and CEO, USSA, and Tom's immediate boss, Randy Andrews (*left*), Founder and President of Andrews International, a wholly-owned subsidiary of USSA. Tom was recognized for propelling his region to an unprecedented almost 300% growth in 2016. Andrews International provides both armed and unarmed private security guarding services in Honduras and neighboring Nicaragua.



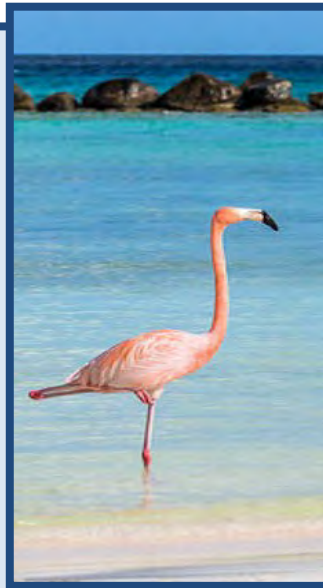
Aruba Beckons

By George Michael Newman

Intellenet's 2018 Annual Membership Meeting in Aruba is expected to be like no other, as the Board once again looks toward providing a unique and educational experience to those who attend.

The island is a constituent country of the Kingdom of Netherlands, and a mélange of cultures resulting from its rich history. Somewhat recently, it was thrust into an extended media focus resulting from the disappearance, in 2005, of Natalie Holloway. It is expected that among the presentations assembled for attendees will be a local authority contributing insights into what became a serial course of complex events that captivated world media for years.

Social media always being an investigative resource, one which surges forward almost at the speed of information



on the Internet, an extended presentation will address then-current and probable future resources. All who practice the art and craft of investigation, in whatever professional realms, will enrich their skillsets and expertise during an informative and entertaining opportunity to learn from one of the field leaders.

And, members from around the world will once again share a wealth of regional knowledge and insights for those instances when a case comes from, goes to or works through their part of the globe.

All in all, with the educational platform combined with the venue, the Aruba conference beckons.



Protecting Human Assets

By Neal Custer

Introduction

When you ask people what is most important to them, their families are usually at the top of the list. Having your credit card number stolen makes for a stressful experience, but it pales in comparison to the feeling of having a child or elderly parent's safety compromised.

Phones for Kids

While the digital advancements we see daily can make life easier, they can also make it more complicated and make the act of maintaining a safe environment far more difficult, especially for parents. As of 2011, one in five elementary school students owned a cell phone. Instead of playing pretend and building sand castles, they are spending recess on Snapchat and Facebook. Many young children are exposed to smartphones as infants; instead of handing their little babies rattles, overstressed mothers are reaching more and more for their phones and tablets.

Arming your 9-year-old with a bright shiny new iPhone might make him the coolest kid on the playground, but it also paints a target on his head for both schoolyard and adult thieves. The expression "taking candy from a baby" becomes far more tempting to a thief when the candy is a \$400.00 boy.

If you're buying a phone for a child, at

least consider what you actually want. Do you just want a reliable means of communication in case of emergency? Non-smart "feature phones" are still widely available from every major carrier, especially for their no-contract



plans. These phones come in a variety of sized and user interfaces: flip phones, Blackberry lookalikes with full keyboards, touchscreens and more. They cost somewhere around \$10.00 for the phone and \$25.00 per month for unlimited minutes. There are no malicious apps to download and no time wasted in class on Facebook.

If you really feel your child needs a smartphone, take precautions. Certain apps have user interfaces more suited to children. A parent sets up the main administrative account, locked with a password, and determines which apps and features the

child can use. The phone is then put into a simple mode that allows only those. The appropriately titled "Kid Mode" by Zoodles (a default on newer HTC phones) is the most commonly seen app of this kind on Android devices.

For iPhones and iPads, consider the options in the "Settings" panel. The "Guided Access" option (Settings>General>Accessibility>Guided Access) allows someone to lock a device to allow the use of only a sign app. All other features are locked until the user enters the correct PIN. This is useful if you load a game on your own device and hand it to your child.

An even more important collection of settings is found in the "Restrictions" panel (Settings>General>Restrictions). This allows an administrator (such as a parent) to control exactly what the device is and isn't allowed to do. Parents can disable in-app purchases, control the types of websites that are available through Safari (or disable it altogether), and limit or remove a child's ability to play games or add friends in the Apple Game Center.

There is one distinct advantage to giving your offspring a smartphone: You now have a GPS tracker on your child, and he or she will never want to leave it behind. Apps like Cerberus,

Continued on next page ...



“Apps like Cerberus, PhoneSheriff, NetNanny and My Mobile Watchdog allow parents to precisely pinpoint a child’s GPS location ...”

PhoneSheriff, NetNanny and My Mobile Watchdog allow parents to precisely pinpoint a child’s GPS location, listen in on her conversation and intercept her communications.

Having access to this information may seem intrusive, but consider: If your child was communicating with a dangerous individual online, you’d be the first to know. In the horrifying possibility of a child abduction, having access to the phone’s GPS location could mean the difference between life and death.

As with any scientific advancements, smartphone technology can be applied positively or negatively. Parents need to be aware of these options to make educated decision about how to approach the smartphone issue with their kids.

Notably, many of these same concepts can also be used to help the elderly, including a parent with dementia or failing health. Keeping track of a parent’s location and helping to block bad web content can prevent your parent from getting scammed or being physically injured. A number of technological advancements are marketed directly at the elderly, such as emergency cellphone wristbands, remote monitoring systems for nursing homes, and most interestingly a special type of desktop computer that provides a simplified user interface for the elderly.

These kinds of computers come with a specific set of advantages and disadvantages, and as with all new technology there are many consumer questions that need answered. Are they really useful? Are they worth the money over a standard computer? What are the alternatives?

Be Wary of Computers Marketed to Seniors ...

It’s hard enough for the average user to stay safe online. For those who don’t fall into the tech-savvy demographic, it can become nightmarish.

While there are plenty of seniors who are passionate about the newest technology, many are content to minimize or eliminate their use of the Internet. A 2014 survey found that while close to 90 percent of millennials own smartphones, the number

drops to under 40 percent of those over age 65.

If you try to persuade an elderly relative into getting more connected with technology, understand that your efforts may be a double-edged sword. While you might feel frustrated that you parents can’t see your latest tweet every 10 seconds, it can be dangerous to throw an inexperienced user into the depts. Of the technological wasteland without the right equipment. Someone just learning to navigate the Internet is a minnow swimming with sharks. The elderly are high-value targets by scammers for this very reason.

The key to getting seniors connected while keeping them safe is to find a happy medium, a device that allows the new user to experience what technology has to offer without creating frustration or danger.

One option is a type of computer designed for the elderly. Companies such as Teikin and The Wow Computer have popped up recently, selling computers with ultra-simplified user interfaces to get seniors performing basic tasks such as sending emails and browsing the web. Telikin claims it’s “the world’s easiest computer.” The Wow Computer advertises that its product is “so easy to use, you won’t have to ask your children or grandchildren for help.”

But do these products do the job? Are they worth the price?

Continued on next page ...

These computers often come in the form of all-in-touchscreen units with large-print icons designed to make navigation easy. If you want to send an email, you just push the big button that says “E-Mail.” Press “Search” and user can open a web browser. It’s all reminiscent of the late-90s AOL interface. It makes basic tasks effortless while preventing the user from feeling that he or she may break something.

What’s under the hood? As it turns out, these machines are similar and share similar prices. The Telikin Elite II holds a MSRP of \$1,249.00.

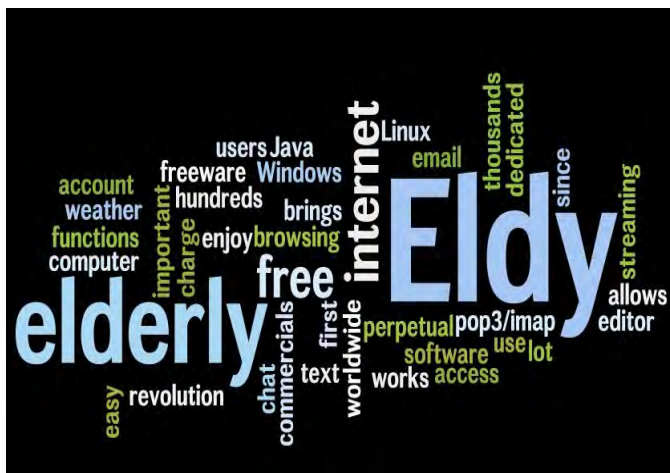
That’s almost as much as a new i7 iMac. If you’re expecting similar components to the iMac, however, think again. The Telikin Elite II comes equipped with an Intel Celeron processor, a 500GB SATA hard drive and a mere 2GB of RAM.

These are extremely low-budget parts for a 2015 computer. A traditional desktop with these same components sell for around \$200.00 at Wal-Mart.

Perhaps the custom operating system justifies the other \$1,049.00? As it turns out, all these machines run version of Linux, the free open-source operating system used on everything from desktops to DVRs. The manufacturer has simply added a user interface to an existing framework.

On the plus side, Linux is generally extremely secure and has a lower malware risk than Windows or Mac

computers. Even so, while these systems may indeed make using the Internet easier for seniors, it’s hard to justify needless sending on old hardware and free operating systems. Everything offered by these machines can be replicated at home for a fraction of the cost.



Because Linux is free, you can legally download your flavor (known as a “distribution”) of choice, burn it onto a CD or DVD, and install it on almost any PC—even one with relatively poor specs. There are even Linux distributions preconfigured for the elder, such as “Ely Linux,” which has the very same kind of simplified, large button interface. With a \$100.00 Craigslist computer and a free copy of Eldy Linux, the same experience of a Telkin can be re-created for next to nothing. Even paying a technology consultant to do the installation is far cheaper than buying a specialized computer for seniors.

Want to try it yourself? The official documentation for Ubuntu, the most common Linux distribution, offers a straightforward tutorial on how to turn a downloaded distribution into a Linux installation disc. Check it out at

help.ubuntu.com/community/burningIsoHowto.

A decade ago, today’s world of Internet-connected refrigerators, wireless battery charging, and the ubiquitous social encouragement to publicly share every thought would have felt like the setting of a science-fiction novel. At the turn of the millennium, the worst trap a user could expect to fall into was replying to an email from a foreign prince wanting to share bank accounts. Today malware can automatically install itself onto a computer, silently conduct a wire transfer, and then use that device to hack somebody else—no prince required.

For seniors, a simplified Linux system might be a viable alternative to a traditional computer both in security and user-friendliness. Read beyond the advertising and examine exactly what you’re buying, or you might waste money on a Pinto advertised as a Porsche. Install Linux yourself or hire a competent tech person to do so, and you’ll end up with a better product at a fraction of the cost.

*Used by permission of the author. **Neal Custer** is an Intellet member and owner of the Custer Agency in Boise, Idaho. He can be reached at neal@custeragency.com. This article will be a chapter in one of Intellet's forthcoming books.*



Truth, Honor and Promises

By Weeden Nichols

Ed. Note: The author served with Intellenet member Bill Blake in the U.S. Army's Criminal Investigation Command. Articles submitted to our newsletter are on the authority of the author. The author addresses universal themes. Reprinted with permission.

Today I propose that we examine a constellation of values concerning honor, statements, promises, agreements, contracts, treaties, and the value of one's word.

Let us start with promises. My understanding is that the making of a promise requires that the promise be kept. Once in a great while, the maker of a promise has to go to the party to whom he made the promise, and state, "When I made this promise, I thought I could keep it, and I had every intention of doing so. Now I find that it is not humanly possible for me to keep this promise. I place it in your hands as to what I must do to make amends." Generally, if one has a good record otherwise, the person to whom the promise was made, will forgive it.

A formal contract is a promise that is legally enforceable. Again, if one has a good record and good will exists in the relationship, the penalty for failure may not be great. If one enjoys a position of power relative to the other party and, to boot, has a brigade of lawyers in his employ, honor still requires that he fulfill the terms of the contract.

A handshake agreement is a contract, perhaps legally enforceable, and perhaps not. It doesn't matter whether it is enforceable or not. Honor requires fulfillment.

One cannot leave a discussion of truth, honor, and reliability without considering national commitments such as treaties and the like. In the current time, we hear declared intentions by a chief executive to disavow treaties already contracted. For the record, I acknowledge that the United States, in the past, has not been entirely innocent of the

use of power to take territory from other nations, to force regime changes, or to force other humiliating concessions upon other nations. I further recognize that the United States of America has reneged on its treaty obligations to Native American tribes, having obtained the concessions the government sought. (Contrast this with Canada's much better record in this regard, having allowed, for example, Colonel James MacLeod to negotiate straightforwardly and in good faith with the First Nations, and then pretty well honoring the treaties he achieved.)

If one is a chief executive of a sovereign nation, and his predecessor has negotiated a treaty with another party (or parties), even if the treaty is not to the new chief's liking, he must abide.

Forcing a "renegotiation" from a position of power is not honorable. Bullying is not honorable. A discussion of possible, mutually acceptable, accommodations to changing circumstances may be reasonable and worth pursuing.

Everyone makes statements in abstract discussions or to support one's own position toward a tangible advantage. Regardless of one's reason for making a statement, if one makes a statement purporting to be a statement of fact, one, in effect, has given his word that he has substantial reason to believe the accuracy of his statement. Before making a statement purporting to be fact, one must have verified its accuracy to the full extent possible. If one is making a statement about another person, particularly one that could amount to libel, one must have, not only a verified reason to believe the statement is fact, but must believe there is an overriding necessity for the disclosing of this verified fact. Not to observe these caveats is dishonorable. In short, stating something as fact is a promise of accuracy.

Sabers or pistols at dawn probably never were suitable remedies for honor violations. Honor is either observed or violated, regardless of who is the best pistol shot or best swordsman, or who had the most money, or who employs the most lawyers. A person without honor deserves the status of pariah, not admiration and respect.





ISPLA News for INTELLENET

By

Bruce Hulme H. Hulme, CFE, BAI

ISPLA Director of Government Affairs

Criminal Record Pre-employment Checks: Update on Restrictions

Investigative and security professionals conducting pre-employment background checks should review this article carefully as it is a trend being proposed in a number of federal, state and local jurisdictions.

The City of New York in 2015 enacted the Fair Chance Act (FCA), which, subject to limited exceptions, prohibits private employers from seeking information from job applicants regarding their past criminal convictions prior to making a conditional offer of employment. Now, two years after the enactment of the FCA, the New York City Commission on Human Rights has finally issued detailed rules and regulations that employers must follow in order to comply with the FCA. They become effective on August 5, 2017.

Subject to limited exceptions, under the FCA, employers with at least four employees are prohibited from asking individuals about any prior criminal conviction until after a conditional offer of employment is made. However, the FCA's prohibitions do not apply:

- To any actions taken by an employer pursuant to any federal, state or local law that requires criminal background checks for employment purposes or bars employment based on criminal history;
- To individuals applying for employment as a police

officer, peace officer or at a law enforcement agency; or

- To individuals applying for a position listed on the website of the New York City Department of Citywide Administrative Services as having been determined to involve law enforcement, be susceptible to bribery or corruption or that entails the provision of services to or safeguarding of individuals who, because of age, disability, infirmity or other condition, are vulnerable to abuse.

The rules and regulations promulgated by the Commission dictate that under the FCA, employers are prohibited from engaging in any of the following actions before making an adverse employment decision concerning an applicant for hire, promotion or transfer:

- Seeking to discover, obtain or consider the criminal history of an applicant.
- Expressing any limitation or specifications based on criminal history in job advertisements, postings or applications. This includes, but is not limited to, any language that states or implies "no felonies," "background check required" or "clean records only."
- Using an application that contains a question about an applicant's criminal history or pending criminal case or requests authorization to perform a background check even if applicants are informed that if they are applying for a position in New York City they can skip the question.
- Making any inquiry or statement related to an applicant's criminal history, whether written or oral, during a job interview.

Continued on next page ...

- Asserting, whether orally or in writing, that individuals with a criminal history or individuals with certain convictions will not be hired or considered.
- Conducting investigations into an applicant's criminal history, including the use of publicly available records or the Internet for the purpose of learning about the applicant's criminal history, whether such investigations are conducted by an employer or for an employer by a third party.
- Disqualifying an applicant for refusing to respond to any prohibited inquiry or statement about the applicant's criminal history; and
- In connection with an applicant, searching for terms such as, "arrest," "mugshot," "warrant," "criminal," "conviction," "jail" or "prison" or searching websites that purport to provide information regarding arrests, warrants, convictions or incarceration information for the purpose of obtaining criminal history.

The rules and regulations state that an employer is not liable under the FCA if it inadvertently learns of an applicant's criminal history without engaging in any of the above actions. However, if the employer uses the inadvertently discovered information to further explore an applicant's criminal history before a conditional offer of employment has been made or uses the information to determine whether to make a conditional offer of employment, the employer will be liable under the FCA.

Further, the rules and regulations state that once an employer has made a conditional offer of employment, the employer may (1) ask, either orally or in writing, whether an applicant has a criminal conviction history; (2) run a background check or, after receiving the applicant's permission and providing notice, use a consumer reporting agency to do so; and (3) ask about the circumstances that led to the conviction and gather information relevant to the Article 23-A factors (discussed below).

If the employer does not wish to withdraw the conditional offer of employment, their obligations under the FCA have been satisfied. If, however, after learning of the applicant's criminal history, the employer wishes to withdraw the offer of employment, the rules and regulations require the employer to (1) engage in an Article 23-A analysis and (2) follow the "Fair Chance Process."

The FCA's rules and regulations also assert that after evaluating the above factors, the employer must then determine whether there is a direct relationship between the applicant's conviction history and the prospective job ("direct relationship exception") or if employing the applicant would involve an unreasonable risk to property or to the safety or welfare of specific individuals or the general public ("unreasonable risk exception"). If, after weighing the above listed Article 23-A factors, an employer cannot determine that either the direct relationship or unreasonable risk excep-

Continued next page ...

Article 23-A of the New York State Corrections Law

This law states that employers may not discriminate against employees or applicants based on their prior criminal conviction without taking into account the following factors:

- a) The specific duties and responsibilities necessarily related to the prospective job;
- b) The bearing, if any, of the conviction history on the applicant's or employee's fitness or ability to perform one or more of the job's duties or responsibilities;
- c) The time that has elapsed since the occurrence of the criminal offense that led to the applicant or employee's criminal conviction, not the time since arrest or conviction;
- d) The age of the applicant or employee when the criminal offense that led to their conviction occurred;
- e) The seriousness of the applicant's or employee's conviction;
- f) Any information produced by the applicant or employee, or produced on the applicant's or employee's behalf, regarding their rehabilitation and good conduct; and
- g) The legitimate interest of the employer in protecting property, and the safety and welfare of specific individuals or the general public.

tions apply, then the FCA prohibits the employer from revoking the conditional employment offer.

If, however, the employer determines that either the direct relationship or unreasonable risk exceptions apply and the employer wishes to withdraw the conditional offer, then the FCA's rules and regulations require the employer to follow the Fair Chance Process by:

Providing a written copy of any inquiry made to collect information about criminal history to the applicant. This includes, but is not limited to, copies of consumer reporting agency reports, print outs from the Internet, records available publicly and written summaries of any oral conversations, specifying if the oral information relied upon came from the applicant;

Providing a written copy of the Article 23-A analysis to the applicant by use of the Fair Chance Notice, which is available on the Commission's [website](#), or a comparable notice;

Allowing the applicant a reasonable time to respond to the employer's concerns (no less than three business days); and

Considering any additional information provided by the applicant during this period.

If the employer ultimately decides to revoke the conditional offer of employment after following the above steps, the employer must notify the applicant in writing. Notably, the above restrictions and requirements

apply not only to individuals with prior criminal convictions but also to those with pending arrests that have not yet been adjudicated.

The FCA's rules and regulations note that there is a *per se* violation of the FCA if an employer takes any of the following actions:

“New York City employers should review their job applications to ensure that they do not seek information regarding individuals’ criminal conviction history.”

- Declaring, printing or circulating, or causing the declaration, printing or circulation of any solicitation, advertisement, policy or publication that expresses, directly or indirectly, orally or in writing, any limitation or specification in employment regarding criminal history. This includes, but is not limited to, advertisements and employment applications containing phrases such as, “no felonies,” “background check required” and “must have clean record.”
- Using applications for employment that require applicants to either grant employers permission to run a background check or otherwise provide information regarding an applicant's criminal history.

- Making any statement or inquiry relating to the applicant's pending arrest or criminal conviction before a conditional offer of employment is extended.
- Using within New York City a standard form, such as a boilerplate job application, intended to be used across multiple jurisdictions, which requests or refers to criminal history. Disclaimers or other language indicating that applicants should not answer specific questions if applying for a position in New York City does not shield an employer from liability.
- Failing to comply with the requirements of the Fair Chance Process, as outlined above.
- Requiring applicants or employees to disclose an arrest that, at the time disclosure is required, has resulted in a non-conviction.

Employers who violate the FCA may be liable for, among other things, compensatory damages (*e.g.*, the wages the individual would have earned had they been hired), punitive damages, attorneys' fees and civil penalties ...

If the Commission finds that an employer's actions were willful, wanton or malicious, the Commission may impose a civil penalty of up to \$250,000.

New York City employers should review their job applications to ensure that they do not seek information regarding individuals' criminal conviction history. Indeed, New York City

Continued next page ...

employers who ask about prior criminal convictions on employment applications must revise those applications to remove such questions. Employers should also review job postings and other pre-hire paperwork to ensure that they do not inquire about or reference information concerning an applicant's prior criminal conviction prior to making a conditional job offer.

ISPLA is grateful to the employment law firm of Fox Rothschild for providing us with this timely information. For more information about this labor law alert, please contact [Glenn S. Grindlinger](mailto:Glenn.S.Grindlinger@foxrothschild.com) at 212.905.2305 or ggrindlinger@foxrothschild.com, [Raquel A. Gutiérrez](mailto:Raquel.A.Gutiérrez@foxrothschild.com) at 646.601.7637 or rgutierrez@foxrothschild.com or any member of the firm's [Hospitality Practice](#).

New Form I-9 Mandatory Effective September 18, 2017

The United States Citizenship and Immigration Services (USCIS is a division of the U.S. Department of Homeland Security) released a revised version of Form I-9, Employment Eligibility Verification, on July 17, 2017. This new edition of the form, will bear a revision date of 07/17/17 N, become mandatory on September 18, 2017, and will replace all prior editions of the form as of that date.

Employers may use either the current edition (with a revision date of 11/14/16 N) or the new edition, once released, through September 17, 2017. However, as of September 18,

2017, only the new edition will be acceptable for new hires or reverifications. The new version of the Form I-9 is expected to include the following changes:



Revisions to the Form I-9 Instructions:

- 1) The name of the "Office of Special Counsel for Immigration-Related Unfair Employment Practices" will be changed to its new name, "Immigrant and Employee Rights Section."
- 2) The phrase "the end of the first day of employment" will be shortened to "the first day of employment."

Revisions Related to the List of Acceptable Documents on Form I-9:

- 1) The Consular Report of Birth Abroad (Form FS-240) will be added to List C.

Employers completing Form I-9 on a computer will be able to select Form FS-240 from the dropdown menus available in List C of Section 2 and Section 3. E-Verify users will also be able to select Form FS-240 when creating a case for an employee who has presented this document for Form I-9.

All of the certifications of report of birth issued by the Department of

State (Form FS-545, Form DS-1350 and Form FS-240) will be combined into selection Item 2 under List C.

- 2) All List C documents, except the Social Security card, will be renumbered.

For example, the employment authorization document issued by the Department of Homeland Security on List C will change from Item 8 under List C to Item 7 under List C.

- 3) All changes will be incorporated into a revised edition of the M-274 Handbook for Employers: Guidance for Completing Form I-9, which is also being revised to make it easier for users to navigate.

All U.S. employers are required to complete a Form I-9 for **every** employee hired in order to verify that the individual is authorized for employment in the United States under the Immigration Reform and Control Act of 1986 (IRCA). **Beginning September 18, 2017, employers must use the new version of the Form for all new hires and for re-verifying current employees with expiring employment authorization documentation.** [Employers should not complete new forms for existing employees who do not require reverification.] A best practice would be for employers to begin using the new edition of the form immediately upon its release.

Form I-9 is used for verifying the identity and employment authorization of individuals hired for employment in the United States. All U.S. employers

Continued on next page ...

must ensure proper completion of Form I-9 for each individual they hire for employment in the U.S. This includes citizens and noncitizens. Both employees and employers (or authorized representatives of the employer) must complete the form. On the form, an employee must attest to his or her employment authorization. The employee must also present his or her employer with acceptable documents evidencing identity and employment authorization. The employer must examine the employment eligibility and identity document(s) an employee presents to determine whether the document(s) reasonably appear to be genuine and to relate to the employee and record the document information on the Form I-9. The list of acceptable documents can be found on the last page of the form. Employers must retain Form I-9 for a designated period and make it available for inspection by authorized government officers. ISPLA suggests that all such Form I-9 material of employees be filed together in a separate file in the event of such government inspections, thus minimizing the potential inspection of an employment file being scrutinized for other infractions that might unknowingly be disclosed in a specific employee's personnel folder.

Concealed Carry Reciprocity Acts Status Report

The American Bar Association has submitted letters in opposition to H.R. 38, the “Concealed Carry Reciprocity Act of 2017” sponsored by Repre-

sentative Richard Hudson (R-NC-8) and S.446, the “Constitutional Concealed Carry Reciprocity Act of 2017” sponsored by Senator John Cornyn (R-TX). The two measures essentially mandate national reciprocity for concealed carry permits issued pursuant to state law. Any state that allows some form of concealed carry – and



all states do – would have to recognize a concealed-carry permit issued in another state. A similar House bill passed in past Congresses when Republicans controlled the House of Representatives, but failed to pass the Senate. The current House bill has 205 cosponsors, 103 Republicans and two Democrats. The Senate version has 38 cosponsors, all Republicans.

It is the ABA's position that such policy offends deeply rooted principles of federalism where public safety is traditionally the concern of state and local government. "A state's ability to consider safety factors—such as age, evidence of dangerousness, live firearm training, or criminal records—would give way to other states' less stringent requirements. Unlike some efforts of Congress to create minimum safety standards, this bill could lead to no safety standards as more

states enact laws to allow persons to carry concealed firearms without a permit."

They point out that knowledge of local authorities, who best know the individual applicant, would also be rendered moot. For example, a person with a history of domestic disturbances, who might be denied a concealed-carry permit in his own state, could simply obtain a permit in another state. Even worse, permits that are revoked, counterfeited, or otherwise invalid would be difficult to identify by law enforcement or other officials who need to know, as there is little means of verifying an out-of-state permit. The growth of “permitless” carry states would only further confound this verification dilemma. For these reasons, the ABA in 2011 adopted policy expressly opposing “federal legislation that would force states to recognize permits or licenses to carry concealed weapons issued in other states.”

They also contend that these proposed bills are unnecessary as the majority of states, through reciprocity agreements, already recognize concealed carry permits issued in selected states. However, these reciprocity agreements are typically between states that have similar concealed carry licensing requirements. The discretion of states to enter, or not enter, into reciprocity agreements is critical to their core public safety function. With the increase in right-to-carry laws across the country, the crime rate has also increased. In June, Stanford Law Professor John Donohue published a study, based on decades

of crime data, corroborating this point. He estimated that “Ten years after the adoption of [right-to-carry] laws, violent crime is estimated to be 13-15% percent higher than it would have been without the RTC law.”

The ABA contends that Congress should not tie states’ hands when it comes to deciding who can carry guns within their borders. How do investigative and security professionals feel about these two bills and the position of the ABA?

Reciprocity and Recognition —

“Streamlining Licensing Across State Lines: Initiatives to Enhance Occupational License Portability”

As I pen this article for the INTELLENET Newsletter in July, the Federal Trade Commission’s Economic Liberty Task Force has not yet held its scheduled upcoming “roundtable” to examine ways to mitigate the effects of state-based occupational licensing requirements. The disparity between states’ licensing statutes can make it difficult for private investigators and security professionals who are state-license holders to obtain licenses in other states. License portability restrictions often prevent otherwise qualified people from marketing their services across state lines or when they move to a new state. The Task Force is considering how occupational licensing reform might reduce barriers to entry, enhance competition, and promote economic opportunity. Reciprocity and recognition of state licens-

es are a factor in this issue.

State licensing rules, by their very nature, may inhibit one’s ability to provide services in a given state. Even in situations where licensing serves a legitimate health and safety purpose, licensing requirements restrict the

“Recognizing the costs to both consumers and licensees of multistate licensing requirements, a variety of initiatives have sought to enhance occupational license portability.”

labor supply and reduce competition, and therefore may increase the price consumers pay for services. Licensing restrictions also may limit employment opportunities for qualified providers. Some states are also in the process of deregulating this profession.

Because licensing rules are primarily state-based, it may be difficult for someone licensed in one state to become licensed in another. State licensing standards vary considerably, thus applicants licensed in one state may need additional education or training to qualify for another state’s license. Even when a profession’s underlying standards are national and state licensing requirements are similar throughout the United States, the process of obtaining a license in another state can be slow, burdensome,

and costly.

The need to obtain a license in multiple states can reduce interstate mobility and practice, and even lead licensees to exit their occupations when they move to another state. The need for multi-state licensure also affects consumers’ access to services. It may prevent qualified investigative and security service providers from addressing time-sensitive emergency situations near state lines, limit the ability of members of our profession to render professional services to our clients or consumers in underserved locations, or areas where experiences investigative or security services are in short supply.

Recognizing the costs to both consumers and licensees of multistate licensing requirements, a variety of initiatives have sought to enhance occupational license portability. New types of models have emerged thus far.

- Some nationwide organizations of state licensing boards for individual professions have developed interstate licensing compacts. These binding contracts are enacted by states to define licensing standards and processes, and to share applicants’ records and disciplinary information among states participating in the compact.
- Other occupational organizations such as International Association of Security and Investigative Regulators (IASIR) have developed agreements, model laws, and model rules that serve many of

the same purposes as compacts. The FTC, IASIR and ISPLA are exploring options for enhancing the portability of occupational licenses. Topics of discussion include:

- Barriers to entry raised by cross-state occupational licensing requirements;
- The law of interstate compacts;
- Licensing portability mechanisms (which may include enabling one state license to be recognized by all states, expedited licensing in additional states, and temporary licensure);
- The status and effectiveness of interstate licensing compacts, agreements, and model laws intended to ease licensing requirements across state lines for specific professions; and
- The potential impact of portability measures on licensee mobility, market entry, provider supply, and competition among service providers.

ISPLA Seeks Input ...

To assist us in our analysis of these issues and various policy proposals intended to address them, ISPLA seeks input from our investigative colleagues on the following questions:

- 1) Is obtaining a license in another state a significant barrier to mobility in your business? If so, what factors contribute to the difficulty – e.g., differences in state standards, burdensome paperwork, multiple fees, etc.?
- 2) To what extent is the increased ability to provide certain services electronically (such as by database information and public record searches) driving greater interest in mechanisms to ease the burdens of multistate licensing?
- 3) What are the advantages and disadvantages of the mechanisms that interstate licensure compacts and model laws use to ease licensing requirements across state lines, such as mutual recognition, endorsement, and expedited licensure?
- 4) How effective are compacts and model laws in reducing barriers to entry in licensed occupations, enhancing mobility of licensees, increasing the supply of licensees, and promoting competition among service providers?
- 5) How does an interstate licensure compact differ from a model law used to streamline licensing across state lines? What factors influence the choice of an interstate compact or a model law to ease cross-state licensing requirements?
- 6) What factors contribute to a successful compact or model law for easing licensing requirements across state lines? Are interstate licensure compacts or other mechanisms more suitable for some occupations than others? Is this an initiative we should pursue?
- 7) To what extent does the effectiveness of a compact or model law depend on harmonization of state requirements for licensing? Do compacts and model laws tend to increase the substantive or procedural standards to obtain a state license? If there is an increase in standards, does that limit licensee participation or otherwise reduce the effectiveness of a compact or model law in easing licensing requirements?
- 8) To what extent do centralized databases of applicants' credentials, criminal background checks, and disciplinary information contribute to the effectiveness of an interstate licensure compact? Do centralized databases make it more likely that the compact will be accepted by licensees and clients of licensees?
- 9) What factors influence a state's decision to enter into a compact or adopt a model law? Are some states more willing to become part of a compact or model law than others? How effective are compacts and model laws that are not universally adopted? How can organizations that develop and administer compacts

“Are interstate licensure compacts or other mechanisms more suitable for some occupations than others? Is this an initiative we should pursue?”

and model laws foster their adoption by more states?

10) What, if anything, can or should the federal government do to encourage adoption of compacts and model laws that promote license portability across state lines?

11) Are there some occupations for which it would be better to reduce or eliminate licensing requirements, rather than develop an interstate licensure compact or model law to ease licensing requirements across state lines? What factors would influence this analysis?

I would be grateful to receive your comments at brucehulme@yahoo.com.

ISPLA and INTELLENET are also a members of the International Association of Security and Investigative Regulators and I serve as the IASIR industry board member representing private investigators. Your



INTELLENET newsletter editor, Don Johnson, also serves on the IASIR board representing the State of Indiana. IASIR is comprised of state and provincial government regulators in the United States, Canada, France and the United Arab Emirates. It is also comprised of three additional industry board members who represent the interests of private security, ar-

mored cars and the alarm industry. This same subject matter will most likely be a major agenda item at its 2017 IASIR Conference to be held in Chattanooga, Tennessee November 8-10 (November 7 Board meeting) hosted by the Tennessee Department of Commerce and Insurance. The venue is the Double Tree by Hilton Hotel Chattanooga Downtown. More information is available at www.IASIR.org.

Please consider donating to [ISPLA](#) to assist in its continuing mission. Bruce can be reached at brucehulme@yahoo.com.



PROTECT YOUR COMPANY

Intellenet, in partnership with Finley Consulting and Investigations, has scheduled a two-day workshop (Protecting Your Business—Are You Prepared?) at the Pittsburgh Marriot North Hotel in Cranberry Township, PA (Pittsburgh area) for Thursday and Friday, September 14-15, 2017. The focus of this workshop will be on responding to questions a business owner may have.

The attendee fee is \$159.00 and includes morning and afternoon drink breaks and a sandwich lunch each day. Registration and fee payments may be made through www.intellenetwork.org. Credit cards are accepted.

Attendees must make their own hotel reservations at (724) 772-3700. The hotel has offered a rate of \$155.34, including tax, internet and a free full breakfast. The room rate cut-off date is August 23, 2017.