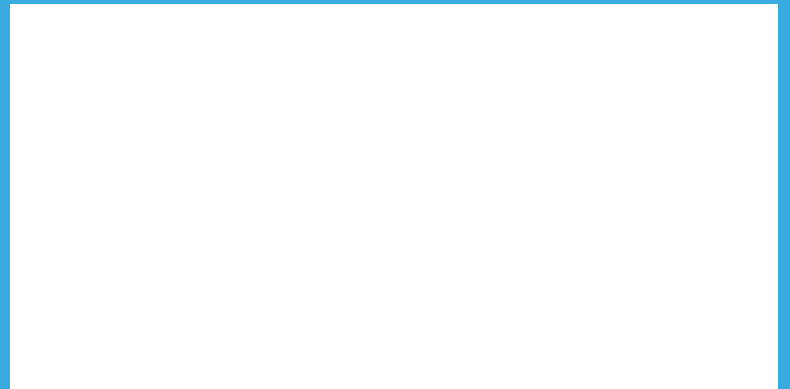


# The Iowa County

magazine



October 2022  
Cybersecurity Month



# THE ROAD TO SUCCESS



## CAT® COLD PLANERS

With a combination of high efficiency and ease of operation, Cat Cold Planers are built to get the job done. Efficient and powerful performance with simplified controls and integrated technology help you finish the job faster with the milling precision you need.

MODEL	OPERATING WEIGHT	MILLING WIDTH	HORSEPOWER	MAXIMUM MILLING DEPTH
PM620	73,480 lbs.	79.1"	630 hp	13"
PM622	74,737 lbs.	88"	630 hp	13"
PM820	79,653 lbs.	79.1"	800.6 hp	13"
PM822	80,910 lbs.	88"	800.6 hp	13"
PM825	82,673 lbs.	98.6"	800.6 hp	13"

VIEW ALL PAVING MACHINES:

[www.zieglercat.com/paving](http://www.zieglercat.com/paving)

**ZIEGLER** 

# The Iowa County

October 2022 \* Volume 51, Number 10

The Iowa County: The official magazine of the  
Iowa State Association of Counties  
5500 Westown Parkway, Suite 190  
West Des Moines, IA 50266  
515.244.7181 FAX 515.244.6397  
[www.iowacounties.org](http://www.iowacounties.org)  
Rachel Bennett, EDITOR

Copyright © 2022 Iowa State Association of Counties  
Statement of Ownership included on page 20

See Yourself in Cyber <i>Chris Judge</i>	4-5
Crowdstrike and Other Resources <i>Jesse Martinez and Jess Flaherty</i>	6-7
Meet Jess Flaherty and Shane Dwyer	7
Cybersecurity Simulation Training - Better than Reality <i>Tim Rahschulte and Rita Reynolds</i>	8-9
The Road (to Cyber Maturity) Goes Ever On <i>Dylan Lynch</i>	10-11
ICIT Paying IT Forward <i>Micah Van Maanen</i>	12-13
Cryptocurrencies and NFTs: Bored Apes and Rich Idiots <i>Anthony Kava</i>	14-15
General Session Minutes Summary	15
Popular Scams <i>Dylan Young</i>	16-17
MS-ISAC Baltimore Conference Report <i>Anthony Kava and Jesse Martinez</i>	18-19
First Annual Certified Iowa County Supervisor Graduation <i>Katie Cook</i>	20-21
Calendar of Events	22



#### **ISAC's Mission:**

To promote effective and responsible county government  
for the people of Iowa.

#### **ISAC's Vision:**

To be the principal, authoritative source of representation,  
information and services for and about county government  
in Iowa.

#### **ISAC OFFICERS**

**PRESIDENT** Richard Crouch, Mills County Supervisor,  
NACo Board Representative

**1ST VICE PRESIDENT** Brian Gardner - Linn County Sheriff

**2ND VICE PRESIDENT** Barry Anderson - Clay County Supervisor

**3RD VICE PRESIDENT** John Werden - Carroll County Attorney

#### **ISAC DIRECTORS**

Carissa Sisson, Franklin County Assessor

Ryan Dokter, Sioux County Auditor

Danelle Bruce, Mills County Community Services

Matt Cosgrove, Webster County Conservation

AJ Mumm, Polk County Emergency Management

Brad Skinner, Appanoose County Engineer

Shane Walter, Sioux County Environmental Health

Micah Van Maanen, Sioux County Information Technology

Brian McDonough, Polk County Planning and Zoning

Kevin Grieme, Woodbury County Public Health

Mary Ward, Cass County Recorder

Tim Neil, Bremer County Supervisor

Linda Zuercher, Clayton County Treasurer

Elizabeth Ledvina, Tama County Veterans Affairs

Carla Becker, Delaware County Auditor (Past President)

Burlin Matthews, Clay County Supervisor (Past President)

Joan McCalmant, Linn County Recorder (Past President)

Grant Veeder - Black Hawk County Auditor (NACo Board)

#### **ISAC STAFF**

William R. Peterson - Executive Director

Lucas Beenken - Public Policy Specialist

Rachel Bennett - Member Relations Manager

Courtney Biere - Office Support Coordinator

Jamie Cashman - Government Relations Manager

Ashley Clark - IT Project Coordinator

Tyler Connelly - Network Administrator

Katie Cook - Member Support Coordinator

Kristi Harshbarger - General Counsel

Molly Hill - Staff Accountant

Brad Holtan - Finance and Program Services Manager

Brandi Kanselaar - CSN Project Coordinator

Beth Manley - Compliance Officer

Tammy Norman - IPAC Program Manager

Brock Ridders - Software Support Specialist

Jacy Ripperger - Marketing Coordinator

Joel Rohne - Technology Service Bureau Program Manager

Chris Schwebach - Software Developer II

Kelsey Sebern - Event Coordinator

Molly Steffen - Program Support Coordinator

Jessica Trobaugh - ICACMP Project Manager/Trainer

Dylan Young - IT Manager/Senior Software Developer

**\*\* The views and opinions expressed in articles authored by  
anyone other than ISAC staff are those of the authors and do  
not necessarily reflect the official policy or position of ISAC.**

ISAC members are elected and appointed county officials  
from all 99 counties. *The Iowa County* (ISSN 0892-3795, USPS  
0002-150) is published monthly by the Iowa State Association of  
Counties, 5500 Westown Parkway, Suite 190, West Des Moines,  
IA 50266. Periodicals postage paid at Des Moines, IA 50318.  
POSTMASTER: Send address changes to [rbennett@iowacounties.org](mailto:rbennett@iowacounties.org). Subscriptions: \$25 per year.

# See Yourself in Cyber

## CISA & Cybersecurity Awareness Month in Iowa

It has been an eventful year in Iowa, and I am excited to be publishing another article in the ISAC Magazine to fill you in on what's going on here in the Hawkeye State. The Cybersecurity and Infrastructure Security Agency (CISA) team has been busy traveling the state providing our no-cost cyber and physical security assessments, training, exercise, and information-sharing resources. As the weather turns a little cooler, we find ourselves in Cybersecurity Awareness Month once again.

**“See yourself in cyber.”** This is the theme for Cybersecurity Awareness Month 2022. This year's campaign theme demonstrates that while cybersecurity may seem like a complex subject, ultimately, it's really all about people. Each one of us can make small steps that add up to a huge impact on our collective cybersecurity. Each one of us has a role to play.

Since 2004, Congress has declared October to be Cybersecurity Awareness Month in the hopes of helping individuals protect themselves online as threats to technology and confidential data become more commonplace. CISA partners with the National Cyber Security Alliance each year and leads a collaborative effort between government and industry to increase cybersecurity awareness both nationally and internationally.

Being cyber smart is an ongoing battle for federal agencies; state, local, tribal, and territorial governments; critical infrastructure owners and operators; not to mention the general public. The prevalence and sophistication of new technologies means everyone has to be more proactive when it comes to cybersecurity. It is a responsibility that never ends.

Luckily, CISA can help.

Hackers don't need to know how much is in your bank account to want to get into it. Your identity, your financial data, what's in your email...it's all valuable. And, cyber criminals will cast as wide a net as possible to get to anyone they can. They're counting on you thinking you're not a target.

So how can you reduce the chances of falling for the scams? Here are four things you can do right now:

- Turn On Multi-Factor Authentication
- Update Your Software
- Think Before You Click - Recognize and Report Phishing
- Use Strong Passwords

When we say, “See Yourself in Cyber,” we mean see yourself in cyber no matter what role you play. As an Iowa county, as an individual, or a consumer,



**Chris Judge**

CISA Protective Security Advisor  
Iowa District  
[www.cisa.gov](http://www.cisa.gov)





# See Yourself in Cyber

---

take the most basic steps to protect your online information and privacy, and you will be significantly less likely to be the victim of a cyber-criminal. You can learn more at: <https://www.cisa.gov/4-things-you-can-do-keep-yourself-cyber-safe>.

Cybersecurity Awareness Month is a good time to draw attention to the myriad of cyber and physical security issues Iowa has faced this year.

We witnessed the Russian government increase its malicious cyber activities following the invasion of Ukraine. We saw an unprecedented multi-national joint cyber advisory addressing vulnerabilities in Apache's Log4j software library. Ransomware continued to be a plague across the state. We saw extreme weather threaten critical infrastructure. We even witnessed the apprehension of a bomb suspect who had planted incendiary devices in multiple locations across Iowa City.

No individual can face all of these varied security issues alone. With this in mind, and due to the vast number of threats impacting our nation and the local events witnessed in Iowa, CISA has now hired a team of advisors that have been busy canvassing the state providing CISA's resources:

- Chris Judge, based out of Iowa, is the State's Protective Security Advisor.
- Chris Cockburn, based out of Missouri, is the new Cybersecurity Advisor currently covering Iowa.
- Chris Maiers is the new Emergency Communications Coordinator for CISA Region 7. Chris is an Iowa Native and was previously Iowa's Statewide Interoperability Coordinator.

During 2022, our local team has been busy working with its cohorts to sustain our trusted and effective partnerships between government and the private sector. Partnerships are the foundation of our collective effort to protect the Nation's critical infrastructure.

Due to Russia's invasion of Ukraine and recent local events in Iowa, we are working hard to support Industrial Control Systems and Ransomware security with our [Shields Up](#) campaign. We remain dedicated to Soft Target Security and Bombing Prevention through CISA's [Operation Flashpoint](#) and local Bomb-Making Materials Awareness Program training events, which we have hosted in multiple counties across the state.

Due to extreme weather events, our team is laser focused on Climate Resilience, and we are conducting a multi-year local study to support the security of Iowa's water systems through our Regional Resiliency Assessment Program that identifies security and resilience issues that could have regionally or nationally significant consequences.

Given the constantly evolving landscape in emergency communications, our team is actively promoting and enhancing emergency communications capabilities via training, exercises, and other forms of technical assistance through the [Interoperable Communications Technical Assistance Program](#), and we can assist with emergency communications projects while planning or during a response to a planned or unplanned event.

Additionally, we have conducted active shooter training, physical and cyber security exercises, and dozens of security assessments, across the state this year. We work diligently to connect our partners with relevant information-sharing resources, such as [HSIN-CI](#) and the [MS-ISAC](#), and [CISA Alerts](#) to ensure our stakeholders have the most current threat information.

If you are interested in learning more about how CISA can support your security and resilience initiatives, please reach out to CISA Region 7 or any member of our local team.

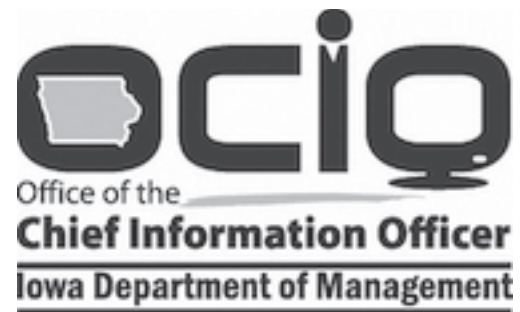
Securing Iowa is a team sport. Let's work together to get it done.

# CrowdStrike and Other Resources

---

Throughout the country, cyber attacks on local governments have severely impacted operations and have resulted in significant financial losses. According to the Center for Internet Security over the last three years, ransomware attacks have more than tripled. As a state, we can do something about ransomware and other malicious activities. Our cities and counties should continue to improve their cyber defenses by deploying IT management patching tools, endpoint protection software, providing staff security awareness training, establishing data recovery tools, and implementing incident response procedures.

The Office of the Chief Information Officer (OCIO) is expanding our support with Iowa counties and is releasing cybersecurity tools and technologies to improve on our state's cybersecurity capabilities. OCIO has been working diligently in identifying funding opportunities that enable cybersecurity services to be provided at no cost to counties. OCIO has a working relationship with every county in Iowa. However, the level of service varies greatly.



**Jesse Martinez**  
Information Technology  
Specialist, OCIO

**Jess Flaherty**  
Local Government  
Program Manager, OCIO

[ocio.iowa.gov](http://ocio.iowa.gov)

---

Ransomware is a concern in regards to cyber attacks on Iowa local government operations and critical infrastructure. Ransomware can be delivered in several ways, including from web browsers, USB devices, and email by using a link or attachment. A ransomware attack on the Colonial Pipeline in May 2021 had devastating consequences on national infrastructure through an exposed VPN password through what investigators believed was an employee using the same password in multiple locations. Preventive measures such as Endpoint Detection and Response (EDR) software are vital to keep attackers out of systems, but are meant to work in conjunction with good cyber hygiene practices like changing passwords and implementing multi factor authentication.

To combat ransomware, OCIO uses and recommends EDR combined with OCIO 24x7 Security Operations Center (SOC) which are effective and critical components in the State of Iowa's overall "defense-in-depth" model. "Defense-in-depth" is a layered approach to implement multiple cybersecurity protections. These protections create multiple layers of defense that reduce the chances that an adversary could successfully damage their target organization. This methodology prevents and will also deter potential attacks.

"We are all in this together. Each of us has a part in improving Iowa's cyber posture while building on our joint capabilities in defending Iowa's government operations against foreign and domestic cyber threats," said Shane Dwyer, the State of Iowa Chief Information Security Officer.

Features of EDR include, but are not limited to, monitoring, alerting, and preventing malicious activity. OCIO is currently preparing to transition to CrowdStrike as the state's EDR solution. Starting in 2023, we will be looking to extend CrowdStrike, a next-generation EDR service, to every county office or department.

CrowdStrike is an award-winning leader in the EDR field. The advanced features of CrowdStrike combined with SOC can substantially improve a county's cybersecurity posture with minimal effort and a phased-in approach.

OCIO's Local Government Program Manager, Jess Flaherty, has been actively engaging county partners on CrowdStrike deployment.

# Crowdstrike and Other Resources

---

“As a state agency we are here to enhance the lives of Iowans. We want to help our local government partners protect the citizens of Iowa. The cybersecurity system allows us to help make cities and counties stronger,” said Flaherty.

OCIO is actively reviewing the other existing cybersecurity services monitored by the SOC and also exploring supplemental tools to strengthen each layer of our defense in depth strategy. OCIO will continue to communicate with county partners on upcoming cybersecurity initiatives and provide situational awareness for the evolving cyber threat landscape.

## Meet Jess Flaherty and Shane Dwyer

---

Jess Flaherty is the OCIO Local Government Program Manager with over 13 years of experience in state government program administration. Prior to joining OCIO, Jess worked at the Office of the Governor and Iowa Finance Authority specializing in project management.



Flaherty completed the Certified Public Manager program at Drake University in 2016 and obtained a Change Manager Practitioner certification from Prosci in 2020. Jess strives to use her skills and experiences to communicate, collaborate, and enhance project implementations to achieve a common goal.

Jess grew up in Indianola but met and fell for a Southern Iowa farmer who relocated her to Clarke County. She currently resides on the farm with her husband and three kids. Jess spends her spare time chauffeuring the kids to all their activities, cheering for the Murray Mustangs, and pretending to help on the farm. She is always looking for small town restaurant recommendations in the region.

Shane Dwyer is the State of Iowa's Chief Information Security Officer and is the principal executive for state-wide Cyber Operations which include data-center services, hosting services, information security services, and networking services.



Prior to his current role, Shane was the Chief Information Security Officer for the Wisconsin Department of Health Services; Senior Director for Information Security at Minnesota State University, Mankato; and was an Operations Manager for the United States Air Force.

Shane holds a Bachelors in Information Systems Security from American Military University and maintains the Certified Information Systems Security Professional, GIAC Security Leadership, and Certified Data Privacy Solutions Engineer certifications.

# Cybersecurity Simulation Training - Better Than Reality

Let's face it, when it comes to some realities it is best to not experience them at all. No one wants to experience a fire in their home or a devastating earthquake, tornado, tsunami, or pandemic. Similarly, no one wants their privacy stolen or the critical assets of their organization threatened. While we would like to avoid risks altogether, we know that they are part of reality; and while nothing tests our readiness quite like reality, we will perform better if we properly prepare.

So, we prepare accordingly. We use risk management protocols to protect and defend against a variety of risks. An example of this is the auto-shutoff switches to our electrical breakers in our homes that prevent a surge in electricity that could cause a fire. We use seat belts to prevent injury from an auto accident. We also use incident response and recovery plans when risks do become reality. Conducting fire drills in schools, offices, and our homes help to prepare us if there is a fire and where we need to respond quickly to protect ourselves and others. We use documented playbooks and manuals sometimes when responding and recovering from a risk-turned-reality because emotions and anxieties can cloud judgement and impair decision making during the chaos of a crisis. It is for similar reasons that we have cyber simulations; we prepare for a reality that we hope never occurs. We prepare because we know the occurrence is very possible, and perhaps, very probable in today's world.

Our understanding of the probability of a cyber risk occurring is similarly high. We know that it is common practice to talk about an inevitable hack, phishing attack, data ransom, or even network sabotage. We also know from security officers, risk managers, and administrators in our community that counties, government agencies, and organizations are not as prepared as they would like to be for the cyberattacks threatening their operations, stakeholders, critical assets, and overall brand. For a variety of reasons (budget, staffing), counties lack fully tested incident response procedures and fully detailed operationalized playbooks ready for use to mitigate cyber threats

and to adequately respond to attacks before they become a crisis. Consider this list of threats. Are you prepared?



**Tim Rahschulte**  
CEO, Professional Development Academy (PDA)



**Rita Reynolds**  
CIO, National Association of Counties (NACO)

[www.naco.org/cyberskills](http://www.naco.org/cyberskills)

A WORLD OF THREATS		
Website defacements	Obtain data left undeleted in cloud	Delete or modify data on public site
Malware-directed internal spying	Blocks access to information system	Computing critical data
Phishing attack	Counterfeit website	Obtain unauthorized access
Compromise mission-critical information	Cause disclosure of sensitive information	Compromise key suppliers' design, manufacturing, or distribution
Network sniffers intercept communications	Exploits weak or no encryption of information	Obtain sensitive data from publicly-available sources
Counterfeit certificates	Malware via email	Wireless jamming
Multi-staged attacks (e.g. hopping)	Malware via removable media	Denial of Service (Dos) attack
Internal and external attack (mixing physical and cyber methods)	Dumpster diving (written passwords left exposed)	Distributed Denial of Services (DDoS) attack
Tampered hardware in supply chain	Software collect network traffic data	Physical attack (e.g. bombing)
Fire	Flood	Hurricane
Earthquake	Pandemic	Tornadoes
Zero-day attack	Data scavenging attacks in the cloud	Exploit vulnerabilities in mobile
Wireless sniffers collect data inside facilities (e.g. key cards)	Physical attack on supporting infrastructure (e.g. cut power)	Subverted individuals placed into organization
Exploit split tunneling (e.g. entering network through laptop on public and secure system simultaneously)	Man-in-the-Middle attack (e.g. third party secretly joins a two-way online engagement)	Exploit multi-tendency in cloud (e.g. observes organizational processes, acquire info, or interfere)
Login/password guessing attack	Hijack IT sessions	Ransomware
Attack timed with critical organizational operation	Malware directs transmission of sensitive information	Third-party violations to policy or procedure accessing information
IoT/SCADA compromises	Insider threat	Software releases with malicious code



# Cybersecurity Simulation Training - Better Than Reality

There are likely many risks on this list that you feel highly confident about addressing if faced in reality. There are likely many as well that you are not very sure about your abilities to face effectively and that you may not even recognize. Finally, there are likely many others that you know for sure that you are not prepared to face with any level of confidence.

In a recent cyber simulation in which we engaged, 48% of participants said they have nothing in place to protect, defend, respond, and recover from a ransomware attack. Another 20% in the study said they had a defense defined, but it has not been tested. No one in the study felt highly prepared in their readiness to experience such a cyberattack.

Collaboration is key to success when facing any of these risks – especially the most riskiest of risks - ransomware. It is for this reason that the NACo County Tech Xchange and the Professional Development Academy have partnered to offer quarterly cyberattack simulations for leaders (<https://www.naco.org/naco-cyberattack-simulation>) – collaborating with one another in a highly facilitated, online program to increase readiness to address the riskiest of risks.

The overriding objective of any cyber simulation is to assess current risk management capabilities among individuals, teams, and key stakeholders. Most simulations assess how well that team of people can detect, defend, respond, and recover from a cyberattack. In addition to people, a well-planned simulation can also highlight readiness of planned processes and use of risk management technologies. In short, the purpose of a simulation is to assess current preparedness to develop action steps that will help close gaps from current state of readiness to a future ready state. That is exactly what these simulations accomplish.

The objectives of each simulation are to:

1. provide a certified test of incident management plans and associated cybersecurity and risk management playbook details aimed to detect, defend, respond, and recover from a cyber risk;
2. baseline current cybersecurity and risk management work capabilities relative to a cyber risk;
3. strengthen the leadership skills of incident managers leading the company through risk planning and incident resolution;
4. improve the quality of the incident management plans and playbook details based on participant engagement in assessments, peer reviews, and best practice benchmarking; and
5. develop immediate action improvement plans to strengthen people, processes, and technical security controls.

Nearly 200 leaders have been collaborating quarterly over the past couple of years to increase their cybersecurity readiness. Thank you for all those who have participated! We encourage others to participate in our quarterly sessions – that are held online and facilitated by expert practitioners. Engagement is 100% FREE! Learn more and enroll today at <https://www.naco.org/naco-cyberattack-simulation>.

INNOVATIVE RECORDS MANAGEMENT FOR OVER 130 YEARS



**Donald Beussink, Account Executive**

c) 319.621.3059 | e) [dbeussink@cottsystems.com](mailto:dbeussink@cottsystems.com)

[cottsystems.com](http://cottsystems.com)



**WE ARE A PROUD SUPPORTER OF ISAC AND IOWA COUNTIES.**

Dorsey's attorneys provide specialized legal services to Iowa counties, including financing, economic development, public health, privacy laws and litigation.

Dorsey & Whitney LLP  
801 Grand, Suite #4100  
Des Moines, IA 50309  
(515) 283-1000



[dorsey.com](http://dorsey.com)

# The Road (to Cyber Maturity) Goes Ever On

---

Cyber maturity is an often-discussed concept in election security. The concept is simple, you start with the foundational elements of cybersecurity and then build and improve. However, the steps to get to cyber maturity are not always clear. They are dependent on your environment, your goals, your abilities, and, of course, the ever-changing nature of security. Cyber maturity is the never-ending goal of cyber and elections security. We wanted to discuss some of the steps our office has taken this year on our road toward cyber maturity.



**Dylan Lynch**  
Elections Cybersecurity Specialist,  
Iowa SOS  
[sos.iowa.gov](https://sos.iowa.gov)

---

First, we continuously work with our state, federal, and private-sector partners for services to assess our systems, networks, and security procedures. For example, we partnered with the Iowa National Guard to conduct an on-site authenticated assessment. For a week, the Iowa National Guard team came to our office to test our systems, see what gaps they found, and what they could do if they exploited those gaps. The Iowa National Guard also conducted threat-hunting activities throughout the year and will do so again on Election Day. We also employ private sector partners to conduct assessments and penetration tests. Finally, we utilize services from the Cybersecurity and Infrastructure Security Agency (CISA), such as their weekly Cyber Hygiene scans. These services test the foundations of cybersecurity and highlight potential next steps.



Second, we created and implemented a vulnerability disclosure program (VDP) for our office. This program makes us the first Iowa state agency and second state election office in the country to have such a program. VDP allows us to utilize the skills and knowledge of ethical hackers to do what they do best, find vulnerabilities. The ethical hackers can act, think, and get in the mindset of malicious actors and by doing so not only test our security, but also our assumptions of our security. VDP has already proven valuable and has led to further discussions into expanding VDP into a full-fledged bug bounty program.

Third, our office and staff have dedicated time and resources to continuing education efforts with the broader cybersecurity and election community. Staff have attended the annual conferences where election security is at the forefront, including: the National Association of State Election Directors (NASSED); the Information Sharing and Analysis Center (ISAC); and the CISA Election Infrastructure Subsector Government Coordinating Council. In addition, staff have presented and shared Iowa's cyber experiences at several conferences over the past year:

- "Talk Nerdy to Me – Cybersecurity Communication" at the National Association of Secretaries of State Conference
- "Vulnerability Disclosure Program" at SecDSM and again soon at Secure Iowa
- "Election Security" at the first ever Left of Boom at ISU in January and the second upcoming event
- "Election Security Bridge Building" and "Election Security Roundtable" at DEF CON

Lastly, we partnered with CISA again to conduct our annual, Iowa-specific Statewide Elections Table-Top Exercise (TTX) in September. While TTX was developed by CISA, the Secretary of State's Auditor Working Group was instrumental in helping guide the scenarios to be relevant, timely, and specific to all 99 county auditors. County auditors were encouraged to invite their local partners like county IT, law enforcement, emergency management, county supervisors, and relevant private-sector partners.

# The Road (to Cyber Maturity) Goes Ever On

Looking ahead, our office will continue to work with our federal, state, and private-sector partners to pursue that never ending goal of cyber maturity. More so, we will continue to work with all 99 county auditors and their partners to secure Iowa's elections. These efforts will include:

- Updating the Election Cybersecurity Administrative Rules with input from partners;
- Retooling how cybersecurity training and information is presented to county auditors;
- Creating better resource and documentation for county auditors; and
- Continuing to work with partners to bring relevant information and resources to county auditors

There will be more on these topics over the next few months. Until then, the road to cyber maturity goes ever on.



**EMPOWERING**  
IOWA COUNTIES

From finance and HR to property tax and document imaging, we deliver powerful software to 50 counties across the state.

[tylertech.com/erp](http://tylertech.com/erp)



**AN IOWA COMPANY  
SERVING  
IOWA COUNTIES**



**FOR COST ALLOCATION SERVICES AND  
FINANCIAL MANAGEMENT SERVICES**

**Contact Jeff Lorenz (515)-238-7989  
or Roger Stirler (515) 250-2687**

## IT Services Meeting Local Needs



**Information Technology**



**Cybersecurity**



**Contracts & Procurement**



[Government.services@iowa.gov](mailto:Government.services@iowa.gov)



[OCIO.iowa.gov](http://OCIO.iowa.gov)

# ICIT Paying IT Forward

---

In December of 2011, Iowa Counties Information Technology (ICIT), in partnership with ISAC, started the “Paying IT Forward” program with a visit to Emmett County. Over the past 11 years, ICIT has assisted over 35 counties with a variety of services including full IT audits, hiring assistance, and IT consulting. Every county we visit is a unique experience, and it has been very rewarding and enjoyable to meet all the great people working in county government. Assisting and educating county employees and elected officials on various IT related topics is at the heart of what ICIT strives to do. With that in mind, I would like to share with you some of the common findings we have seen at the counties we have visited.



**Micah Van Maanen**  
IT Director, Sioux County  
[micaahvm@siouxcounty.org](mailto:micaahvm@siouxcounty.org)

---

## IT in a Silo

When a county does not have a dedicated in-house IT professional, each department takes it upon themselves to make sure their employees can do their job. This often leads to technology decisions being made by that department, for that department, and without consideration of the county as a whole. This is certainly not the fault of those department heads or elected officials. Their primary job is to ensure their office can serve the public to the best of its ability. But this approach is very inefficient in terms of the broader IT infrastructure. There are often departments that have the latest IT technology, while other departments are running outdated equipment and software. Very little thought is then given to network wiring, servers, firewalls, wireless, and a host of other critical IT infrastructure.

Ideally, IT would be handled centrally by an IT professional who is dedicated to making sure that county dollars are spent for the good of all employees. That person can plan, secure, and update all departments and ensure that all departments have up-to-date technology. This will lead to more productive county employees. It will also allow department heads and elected officials to spend their time performing the job they were hired or elected to perform, which ultimately is the best way to serve our citizens.



## No Watchmen on the Walls

In ancient times the watchmen would have the great responsibility of keeping an eye on the horizon and warning the city if there was danger. So too, IT professionals are responsible for ensuring that the county is best prepared for danger. There are free resources available to assist Iowa counties. But free does not mean that they operate without anyone watching them.

The State of Iowa Office of the Chief Information Officer (OCIO) office has free vulnerability scanning. This can assist you in knowing whether your computers are staying up-to-date. Your county may have a vendor that you contract with to install updates. Is anyone verifying that those updates are properly installed? Is anyone available to read and interpret the reports from the vulnerability scanning?

OCIO also has free advanced malware protection that can be installed on all county computers. Because OCIO has a 24x7 Security Operations Center (SOC), they can contact you if a machine is infected. Is anyone verifying that this software is installed? Is anyone available to respond to security alerts?

We have all heard of ransomware attacks, and one of the best defenses for those is a robust backup and recovery solution. You have probably heard us talk about backups too many times, but almost every county we visit has a disaster of a backup solution in place. Using external hard drives sitting on top of a server is not a backup plan.



# ICIT Paying IT Forward

If you are not regularly testing file restores, you do not have a backup plan. If you do not have a copy of your backups offsite, you do not have a backup plan. If you don't have a backup provider or in-house IT professional managing your backups, get one, today. Here are several good questions you can ask yourself or your backup provider:

- Is all our data being backed up?
- How often is our data backed up?
- How long is our backup retained?
- How long will it take to restore our server(s)?
- How long can we afford to be down?
- How much work can we afford to lose (i.e. one day, one hour, one minute)?
- How are our backups protected from ransomware?
- Where will we serve the public if the courthouse (or other county building) is unavailable?
- Who will manage the recovery in the event of ransomware or natural disaster?



Backup and recovery systems are not free, but your data is invaluable. Benjamin Franklin said "An ounce of prevention is worth a pound of cure," and this is absolutely true when it comes to backups. Spend the money today for a robust backup and recovery system so that you don't need to pay more money down the road for recovery of lost or stolen data. Then you can rest easy knowing that you are protected.

If you are interested in having ICIT assist you, please reach out to Joel Rohne, ISAC Technology Service Bureau Program Manager - [jrohne@iowacounties.org](mailto:jrohne@iowacounties.org); or Andrew De Haan, ICIT Technology Advocate - [adehaan@marioncountyiowa.gov](mailto:adehaan@marioncountyiowa.gov) for more details.



**Healthy Eyes.    Healthy Smile.**

**Healthy You!**

 **DELTA DENTAL®**

deltadentalia.com

# Cryptocurrencies and NFTs: Bored Apes and Rich Idiots

---

Last May, actor Seth Green forked over \$200,000 for the right to say he owns a digital picture of an ape. Predictably, his NFT (non-fungible token) was stolen just when the pixelated primate was due to star in a groundbreaking television series. With an Emmy at risk and a murky copyright dilemma at hand, it looked like the show would not go on. In the end, the ape was returned...for a fee of \$300,000. The half million-dollar simian is safe and sound.

Millions of years of progress. Thousands of years of civilization. Hundreds of years of enlightenment. All building to this moment. Some say this is the future of art. Others say it's a fad. I say it's depressing. I want to love this stuff. I want to order sushi with Bitcoin and collect digital plates from Franklin Mint. I don't want to be a cyber-curmudgeon, but here we are.

Non-fungible tokens are essentially digital receipts stored on a blockchain, a digital ledger that records transactions. Anyone in the world with the requisite know-how can see that you, in fact, hold bragging rights to a particular NFT, and these creations can sell for hundreds of thousands of dollars – or at least they did – on OpenSea, an NFT market with billions in trades since 2021. This summer, however, business fell by 99%. OpenSea seems to be in the same boat as crypto.

A Bitcoin is worth \$22,000 right now (though maybe not in five minutes), down 50% from last year. Fluctuating value is a problem, but cryptocurrencies can do magical things like enable person-to-person transfers and transaction fees so low you can make micropayments, e.g., tipping a blogger 25 cents. Smart contracts also have amazing potential. For example, a car dealer could code a crypto bill-of-sale such that when a buyer's money arrives, they get an NFT title, an order is sent to the manufacturer, and payment is released to the factory. All safe, secure, and automated.

But with crypto, and in general, the best way to make money has always been by grifting, and pump-and-dump schemes are alive and well. Plus, now, anyone can mint a coin or an NFT. Remember "Squid Game"? At the height of its popularity, con-artists launched a Squid Game token to cash-in on the meme. They minted and held onto a bunch of initially worthless coins. Then they used spam to create hype which led to a meteoric rise in value from a penny each to \$2800 in one month. That's when the scammers pulled the rug out and made off with \$3 million. The price plummeted to \$0.003 in hours.

Have qualms about swindling? There's another time-honored financial strategy: Luck. Did you know there are chain-vaping teenagers in basements worth more than you'll ever earn? These pint-sized Warren Bro-fets slammed a purple-flavored energy drink, bought some obscure asset when it was just a novelty, and unloaded it at the right time. It can happen, but it's hard to do on purpose. For every millionaire winner there are thousands of nameless losers.



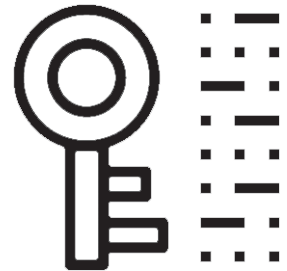
It's tough to call these investments without a way to evaluate or in many cases understand what we're buying. With NFTs, it's even hard to know what is real. OpenSea all but admitted this year that 80% of tokens minted using their free tool are imitations or outright plagiarisms. This came after insider trading allegations in 2021 that an OpenSea exec parlayed knowledge of which NFTs were about to be featured on their site to buy low and sell high.



**Anthony Kava**

Pottawattamie County Sheriff's Office  
[akava@sheriff.pottcounty-ia.gov](mailto:akava@sheriff.pottcounty-ia.gov)

---



# Cryptocurrencies and NFTs: Bored Apes and Rich Idiots

There's still hope. Blockchains have intriguing applications for things that actually belong on a ledger. Though, for better or worse, we're going to need government guarantees. Our anarchist brethren hate to hear it but having the state as arbiter in property disputes has been handy these past couple millennia, and we'll never successfully make the leap to new systems until they're every bit as trustworthy as what we have now. Nor should we.

Current apps are solving problems we don't have with tech that's still evolving. We need to be smart, so we don't put all our eggs in the next Betamax basket. This still feels like a gamble, and today, it's roulette. I wish it were at least poker. We're not there yet, but please stay tuned.

## General Session Minutes Summary

### Summary of Minutes – 2022 ISAC Annual Conference General Session – August 24, 2022

ISAC President Richard Crouch called the 2022 ISAC Annual Conference General Session to order and led the membership in the Pledge of Allegiance. He introduced the ISAC Executive Committee and the remainder of the ISAC Board of Directors.

Bill Peterson gave conference announcements.

Bill introduced NACo 1<sup>st</sup> Vice President Mary Jo McGuire, Commissioner, Ramsey County, Minnesota. Commissioner McGuire addressed the audience.

Lindsey Laufersweiler, Webster County Recorder, awarded the 2022 ISAC Excellence in Action Award to the Clinton County Resource Center and Grow Solar Linn + Johnson Counties. Representatives accepted the award.

Bill Peterson explained the history and qualification of the ISAC Golden Eagle. Grant Veeder, Black Hawk County Auditor, recognized the 2022 ISAC Golden Eagle, Melvyn Houser, ISAC Past President and Pottawattamie County Auditor. Melvyn gave an acceptance speech, and Bill Peterson honored Melvyn as well.

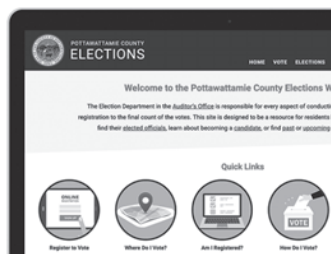
President Crouch adjourned the meeting following conference announcements.



**Website Development  
for Iowa Counties**

Brian McMillin, President  
[brian@neapolitanlabs.com](mailto:brian@neapolitanlabs.com)  
(515) 999-5221

[neapolitanlabs.com](http://neapolitanlabs.com)



# Popular Scams

---

It seems like every day we are being bombarded with odd phone calls, sketchy sounding voicemails, unexpected emails, text messages from unknown sources, or some form of deceiving advertisement. By now you have probably heard from your IT department as if it's on a broken record, that you should not click any links in emails that look suspicious, especially if you were not expecting the email. You know now that doing so could put you or your organization at risk of receiving some form of malware or virus that could take over your entire network, steal your information, and put your important data at risk of being lost forever. But what happens if you get a phone call with the caller identifying themselves as a legitimate sounding business, or perhaps, you get a legit looking email that has no suspicious links in it but only a phone number to call?



**Dylan Young**  
IT Manager/Senior Software  
Developer, ISAC  
[dyoung@iowacounties.org](mailto:dyoung@iowacounties.org)

---

Have you ever wondered who is on the other end of that call, and what would happen if you did get connected with them? In this article we will be highlighting two scams that are popular right now that are scamming people out of money every day. We will learn what they are, what happens, and ways to identify them.

## The Tech Support Scam

Today everyone is doing increased activities online. We now are shopping, banking, connecting with friends and family, and even working online. In the event that something may happen to our device that could interfere with us being able to do any of these things, it could make us react quickly in order to have the issue fixed. The tech support scam preys on this weakness by sparking fear that something is wrong and needs immediate attention.

You may find yourself wrapped up with a tech support scammer in many ways. Perhaps, you received an unsolicited call from someone posing as a legit tech company, like Microsoft, telling you there is an issue with your computer. Or maybe you received an email saying your virus protection software subscription is expired, your computer is at risk, and that you must call them to reactivate the subscription.

Maybe you would be able to determine if these were valid or not, but what if when you were just browsing the web, your computer pops up a message telling you that your computer has a security issue and your social media account(s) and bank account(s) are at risk. Or maybe you were just Googling for a company's support number, and you got the number from one of the first few search results. Yes, scammers today are being rather clever and are paying for advertising on platforms such as Google to have their scam phone number listed.



So, what happens once you get in touch with them? They often will tell you that your computer has been "hacked" or your accounts have had suspicious activity. Regardless, they will say something about getting you connected to their "secure server" so they can take a look at your device. In this process, they are guiding you to install remote software such as AnyDesk, TeamViewer, or UltraViewer. Once they gain remote access, they will typically run a bunch of bogus commands with foreign addresses that can look scary to a non-technical person. This is all part of the tactic to visually convince you there is a problem with your device.

Assuming the victim is still buying into their hoax, they will then either offer to "fix" the issues for some form of payment or try to sell you software that you don't actually need that could even be harmful. They may have a form for you to fill out to purchase the software, but usually they are just taking note of your credit card information at this time. They may ask for payment in forms of cryptocurrency or even gift cards. Let these two payment methods be a big red flag as this is just a way to better hide and launder the stolen money.



# Popular Scams

---

If you did pay them, you now have become one of their “customers”. They often will try other scams to sell you more software and services later down the road. If you denied the scammer at this point, they could become enraged and do things to harm your computer if they still have remote access. If you ever did get into contact with one of these scammers, please go through your programs and uninstall anything they may have installed.

To avoid this scam it's best to ignore unknown calls and texts and know that companies like Microsoft will never reach out directly to you. If you are looking for a company's phone number, it's best to find it on their app or website that you use regularly instead of relying on search engine results.

## **The Overpayment “Refund” Scam**

Much like the tech support scam, you may find yourself wrapped up with a refund scammer in the same way. Often you may receive an email or phone call stating your subscription to something you didn't think you had (because you don't) has been renewed and your account has been charged for it, or they are telling you that purchases for specific items were made on your account. They are leading you to calling that fake support number.

Once you are connected, they will want to know the amount that was “charged” and if you would like to cancel this subscription or get your money back. Of course, everyone wants to get their money back on something they didn't authorize to be purchased. This is where the scam starts. They will tell you in order to process your refund and get your money right away, you must connect to the Company's “secure server”. Sound familiar? Once they are remotely connected to your device, they will typically have you login to your bank account wanting you to write down your balance so you can verify you get the refund once it's processed. The whole point of this is so the scammer can see how wealthy or unwealthy you are for the next part of the scam. Once you do that, they will say in order to process your refund you will need to fill out the refund form. Depending on the scammer, you may be filling out a Google form that they created, or they may just pretend to create a form on the Windows command prompt. The scam comes into action when the victim is asked to enter the amount to be refunded on the fake refund form. When the victim is typing in the amount that they think should be refunded, the scammer, who has remote access, will type extra digits to make the refund amount larger than it's supposed to be. When they had you login into your bank in the beginning, the idea was to see how much money you have so they can determine how much money to steal. After the scammer increases the refund amount and pretends to submit the refund form, they start to act as if something really bad has happened. They will make you feel like you did something wrong and blame you for typing in the incorrect refund amount.

They will tell you that you need to see if you got the transaction by going back into your banking account. With the remote software installed, the scammers can hide the victim's screen so they can't see what the scammer is doing. The scammer will usually transfer the increased refund amount from the victim's savings account to their checking and alter the HTML on the webpage to make it appear as if the refund amount actually went through. Their tactics here is nothing but a visual trick. The victims will see with the edited HTML that it appeared they got the refund, but of course the refund was way too much. The scammer likes to make the victim compare their previous bank balance with the “new” balance to further sell the idea that this actually happened. They will usually give you a deceptive story that they could lose their job for this mistake, and they need your help to correct it. If the victim falls for the scam, the scammer will ask for payment to get the “extra money sent” back. Again, they usually like to stick to getting the money back by having the victim buy gift cards or send cryptocurrency. In some situations where the “extra refund amount” is large enough, they may have you send cash or wire money.

To avoid this scam, it's also best to ignore unknown calls, texts, and emails. If someone is telling you that you have been charged for something, it's best to contact your bank to verify if the transaction actually happened or not. Fraudsters and scammers continue to come up with new ways to take innocent people's money every day. Don't fall into their traps. If you are ever in a situation that just doesn't feel right, question it. Asking simple questions to someone who claims to work for a company can quickly reveal the deception. And as always, please make sure you are verifying email addresses and phone numbers you are calling or receiving. Don't get scammed!

# MS-ISAC Baltimore Conference Report

---

This year marked the 15th Multi-State Information Sharing and Analysis Center (MS-ISAC) Annual Meeting. The in-person event was held in Baltimore, Maryland, and featured seasoned presenters and panelists speaking to the cybersecurity conference theme of “Connect, Secure, and Mature.”

The 2022 Annual Meeting was a multi-day event providing U.S. State, Local, Tribal, and Territorial (SLTT ) government organizations and election officials with a role and interest in information technology operations and security an opportunity to connect and collaborate with their peers and industry leaders on best practices and industry trends. The Annual Meeting included an engaging and informative agenda consisting of contemporary sessions developed by our peers to address topics of greatest interest and relevance to us and the security of our organizations.

In addition to the agenda, the event enabled an unparalleled level of collaboration among peers with whom we were able to both learn from and share our knowledge with. The networking opportunities of MS-ISAC membership are a high-value add to an already high-value event.

MS-ISAC is a trusted cybersecurity partner for over 13,000 organizations including: SLTT government organizations; U.S. State and Territory Homeland Security Advisors; and DHS-recognized Fusion Centers and local law enforcement entities.

The mission of MS-ISAC is to improve the overall cybersecurity posture of SLTT government organizations through coordination, collaboration, cooperation, and increased communication.

There certainly was a great deal of information communicated during dozens of lectures, panels, and other sessions in Baltimore. The diverse line-up of speakers hailed from all areas of government as well as the private sector. This provided those of us from Iowa with important perspectives from other states and counties facing the same challenges as us. While the breadth of topics was almost overwhelming, common strands tied them all together.

First and foremost was an increased focus on election security. The conference was jointly hosted with the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), and they facilitated a dedicated elections track. Threats local officials must consider in 2022 go beyond cyber concerns like intrusions and malware to include foreign influence and physical safety.

One vital tactic we can all use to combat misinformation is to actively engage with our citizens, through both traditional and social media, to provide a transparent, truthful look into how we conduct secure elections. We can and should be a trusted source of impartial information for the public. If we aren't, then others, perhaps with questionable agendas, will fill that void.

We also need to ensure that we not only have incident response plans in place but that we are testing those plans with table top exercises. Drilling, finding things we forgot to include, and revising our playbooks will pay dividends in a real disaster. We really, really don't want the night of a general election to be the first time we get a close look at our emergency procedures.

## **Anthony Kava**

Pottawattamie County Sheriff's Office  
[akava@sheriff.pottcounty-ia.gov](mailto:akava@sheriff.pottcounty-ia.gov)

## **Jesse Martinez**

Information Technology Specialist, OCIO  
[ocio.iowa.gov](mailto:ocio.iowa.gov)

---



# MS-ISAC Baltimore Conference Report

Many experts reiterated the importance of fundamentals in cybersecurity. We like to talk about next-gen firewalls and penetration tests where mock adversaries try to hack into your network, but these things are superfluous if we don't even have an inventory of our systems. Our main job is resiliency. We need to know that we can recover after an attack. That's not always glamorous, but it's also not necessarily complex and expensive. Fundamentally, it means not just doing backups but also testing them and having a proven plan to rebuild from scratch.

Cloud adoption was another recurring theme. Cloud-based services have been fully embraced by the private sector, and they are being slowly adopted in government circles. We can realize amazing benefits, but not all cloud platforms are the same. Protecting our sensitive data takes planning and research. Moving to the cloud can be positive but shouldn't be rushed.

Finally, there were all the lessons learned from COVID-19. Agencies discovered remote work was not just possible but sometimes even preferable. It was a challenge. In the end, it proved theories about how public services could be provided in other types of disasters. If we were able to make things work in a pandemic we needn't fear more mundane disruptions. (And, thankfully, a great many public officials finally learned how to unmute themselves in Zoom.)



Contact Speer today:  
**Maggie Burger, Sr. Vice President**  
[mburger@speerfinancial.com](mailto:mburger@speerfinancial.com)

Helping Counties Navigate:

- ◆ Bond Issues
- ◆ Debt Planning
- ◆ TIF Projects
- ◆ Continuing Disclosure
- ◆ Debt Refinancing



**MAKE**

**Speer Financial, Inc.**

**Your Municipal Advisor TODAY!**



# First Annual Certified Iowa County Supervisor Graduation

The Iowa State Association of County SUPERVISORS (ISACS) is very excited to announce the first ever graduating class of the Certified Iowa County Supervisors continuing education program. The graduating supervisors were recognized in front of their peers at a ceremony held on Thursday, August 25, during the 2022 ISAC Annual Conference.

The program was created and is administered by county supervisors for county supervisors to create a culture of Iowa county supervisor leadership development through a well-rounded continuing education program with the overall goal of bettering county government in Iowa through education. Certification requires a two-year commitment and a total of 30 total credit hours.

We would like to congratulate the 70 graduating supervisors for their hard work and dedication to furthering their education. Congratulations, Certified Iowa County Supervisors!

A special thank you goes out to the Supervisors Continuing Education Committee, Supervisors Executive Board, and the few original supervisors who had the vision to make this happen. We can't thank you all enough for the time, thought, and effort that was put forth to make this program a success.

Registration is now open on the ISAC website, [www.iowacounties.org](http://www.iowacounties.org), for first-time certification and recertification which will run from January 2023 through August 2024. It's free to register, and continuing education credits are offered during events held by the supervisors affiliate and ISAC. Supervisors can also apply for credits when they attend outside events – both in-person or online.



**Katie Cook**

Member Relations Coordinator, ISAC  
[kcook@iowacounties.org](mailto:kcook@iowacounties.org)

## United States Postal Service: Statement of Ownership, Management and Circulation

1. Publication Title: The Iowa County magazine
2. Publication Number: 0892-3795
3. Filing Date: 9/23/2022
4. Issue Frequency: Monthly
5. Number of Issues Published Annually: 12
6. Annual Subscription Price: \$25
7. Complete Mailing Address of Known Office of Publication:  
5500 Westown Parkway, Suite 190, West Des Moines, IA 50266  
Polk Co. Contact Person: Rachel E Bennett  
Telephone: 515.244.7181
8. Complete Mailing Address of Headquarters or General Business Office of Publisher: Iowa State Association of Counties, 5500 Westown Parkway, Suite 190, West Des Moines, IA 50266
9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor: Publisher- Iowa State Association of Counties, 5500 Westown Parkway, Suite 190, West Des Moines, IA 50266. Editor- Rachel E. Bennett, Iowa State Association of Counties, 5500 Westown Parkway, Suite 190, West Des Moines, IA 50266
10. Owner: Full Name- Iowa State Association of Counties.  
Complete Mailing Address- 5500 Westown Parkway, Suite 190, West Des Moines, IA 50266
12. Tax Status: Has Not Changed During Preceding 12 Months
13. Publication Title: The Iowa County magazine
14. Issue Date of Circulation Data Below: 08/31/2022
15. A. Total Number of Copies: Average-2,100, Recent Issue- 2,100 B1. Paid/Requested Outside - County Mail Subscriptions Stated on Form 3541: Average-1,855, Recent Issue-1,850 B2. Paid In-County Subscriptions Stated on Form 3541: Average-72 Recent Issue-65  
C. Total Paid and/or Requested Circulation: Average-1,928, Recent Issue-1,915  
F. Total Distribution: Average-1,928 Recent Issue-1,915  
G. Copies Not Distributed: Average-172, Recent Issue-185  
H. Total Sum: Average-2,100, Recent Issue-2,100  
I. Percent Paid and/or Requested Circulation: Average-100%, Recent Issue-100%
16. Publication Statement of Ownership: Publication Required. Will be printed in the 10/01/2022 issue of this publication.
17. Signature and Title of Editor, Business Manager or Owner: Rachel E. Bennett, Editor. Date: 9/23/2022



# First Annual Certified Iowa County Supervisor Graduation

---



## 2021-2022 Graduates

Barry Anderson, Clay County  
Alan Armstrong, Page County  
Scott Belt, Pottawattamie County  
Al Bloemendaal, Sioux County  
Tom Broeker, Des Moines County  
Peter Buschmann, Delaware County  
Mark Campbell, Webster County  
Dan Campidilli, Hamilton County  
Steven Clark, Dickinson County  
Niki Conrad, Webster County  
Richard Crouch, Mills County  
Tom Determann, Clinton County  
Latifah Faisal, Story County  
Marcus Fedler, Washington County  
Stephanie Hausman, Carroll County  
Lisa Heddens, Story County  
Jean Heiden, Crawford County  
Karl Helgevold, Wright County  
Jodie Hoadley, Adair County  
Colby Holmes, Ringgold County  
Dale House, Van Buren County  
Jeffrey Ives, Pocahontas County  
Scott Johnson, Carroll County  
Sharon Keehner, Clayton County  
Jerry Klobberdanz, Hamilton County  
Dean Kluss, Wright County  
Steve Knapp, Ringgold County  
Erich Kretzinger, Boone County  
Marc Lindeen, Henry County  
Sandy Loney, Humboldt County  
Abigail Maas, Iowa County  
Jeff Madlom, Delaware County  
Burlin Matthews, Clay County  
Lonnie Mayberry, Mills County  
Renee` McClellan, Hardin County

Larry McDevitt, Jackson County  
Crystal McIntyre, Warren County  
Eugene Meiners, Carroll County  
Chuck Morris, Page County  
Jerry Muilenburg, Sioux County  
Linda Murken, Story County  
Heidi Nederhoff, Grundy County  
Tim Neil, Bremer County  
Clayton Ohrt, Buchanan County  
Jerry Parker, Wapello County  
Rick Rasmussen, Wright County  
Donna Robinson, Montgomery County  
Ned Rohwedder, Jones County  
Ty Rosburg, Crawford County  
Richard Ruggles, Carroll County  
Dee Sandquist, Jefferson County  
Charla Schmid, Montgomery County  
Tim Schumacher, Emmet County  
Donald Seams, Wayne County  
Jack Seward, Jr., Washington County  
Garry Seyb, Lee County  
Don Shonka, Buchanan County  
Dan Skelton, Clay County  
Kyle Stecker, Kossuth County  
Jeff Thee, Dickinson County  
Matthew Ung, Woodbury County  
Jayson Vande Hoef, Osceola County  
Carl Vande Weerd, Sioux County  
Shirley Vermace, Winneshiek County  
Carol Vinton, Mills County  
Jerry Walker, Adair County  
Chad White, Henry County  
Jack Willey, Jackson County  
Richard Young, Washington County  
Rick Young, Hamilton County



**Sidwell**  
A Division of HARRIS

**Helping Iowa Counties  
Map Their Future**

With over 90 years of experience, Sidwell is an industry-leading geospatial solutions provider. Let us help you enhance and modernize your GIS!

 [www.sidwellco.com](http://www.sidwellco.com)

 [info@sidwellco.com](mailto:info@sidwellco.com)

 **esri** Partner Network Gold



**Vanguard Appraisals, Inc.**

**For All Your Assessment Services**

- Consultation
- Appraisals
- Software
- Web Sites



**1-800-736-8625** [www.camavision.com](http://www.camavision.com)



## 2022 Calendar



**CENTER**  
for Infrastructure & Economic  
Development

**Renewable Energy Resource for  
Local Leaders**

[www.centerforlocalpolicy.org](http://www.centerforlocalpolicy.org)

### October 2022

9-12 Assessors Fall School  
(Airport Holiday Inn, Des Moines)

### November 2022

10 ISAC Board of Directors Meeting  
(Hilton Downtown Des Moines)

### December 2022

13-16 ISSDA Winter School  
(Holiday Inn Des Moines Airport)

14-16 ICEA Conference  
(Veterans Memorial Community Choice Credit  
Union Convention Center, Des Moines)

### January 2023

18-19 New County Officer's School  
(Sheraton West Des Moines Hotel)

### February 2023

2 Statewide Supervisors Meeting  
(Embassy Suites Des Moines Downtown)

### March 2023

9-10 ISAC Spring Conference  
(Veterans Memorial Community Choice Credit  
Union Convention Center, Des Moines)

### August 2023

23-25 ISAC Annual Conference  
(Veterans Memorial Community Choice Credit  
Union Convention Center, Des Moines)

If you have any questions about the meetings listed above or would like to add an affiliate meeting to the ISAC calendar, please contact Kelsey Sebern at [ksebern@iowacounties.org](mailto:ksebern@iowacounties.org).

### **2022 ISAC Preferred Vendors**

#### **Endorsed Elite Preferred Vendors**

County Risk Management Services, Inc.  
representing ICAP and IMWCA  
Group Benefit Partners

#### **Elite Preferred Vendors**

IP Pathways  
Summit Carbon Solutions

#### **Endorsed Platinum Preferred Vendor**

Iowa Public Agency Investment Trust  
(IPAIT)

#### **Platinum Preferred Vendors**

Ahlers & Cooney, P.C.  
Community State Bank  
D.A. Davidson Companies

Delta Dental  
Henry M. Adkins and Son  
MidAmerican Energy  
Northland Securities, Inc.  
Office of the Chief Information  
Officer (OCIO)  
Schneider Geospatial  
Tyler Technologies

#### **Gold Preferred Vendor**

Cost Advisory Services, Inc.  
Cott Systems  
Custom Tree Care  
The Center for Infrastructure and  
Economic Development  
Dorsey & Whitney LLP  
ISG  
Kofile  
Neapolitan Labs

Purple Wave Auction, Inc.  
Out Services Group  
Sidwell  
Speer Financial, Inc.  
Wellmark Blue Cross Blue Shield of  
Iowa  
Vanguard Appraisals, Inc.  
Ziegler CAT

#### **Silver Preferred Vendors**

Advanced Correctional Healthcare  
ITC Midwest

#### **Endorsed Preferred Vendors**

National Association of Counties  
(NACo)  
Nationwide Retirement Solutions  
Omnia Partners  
Professional Development Academy





**Ryan S. Smith**  
**515.509-2121**  
[rsmith@schneiderGIS.com](mailto:rsmith@schneiderGIS.com)



**Sarah Dickmeyer**  
**515.446.9695**  
[sdickmeyer@schneiderGIS.com](mailto:sdickmeyer@schneiderGIS.com)



**Agland**<sup>TM</sup>  
 Automates assessment  
 calculations



**Beacon**<sup>TM</sup>  
 Blending searches  
 reports, and maps!



**GeoPermits**<sup>TM</sup>  
 Online, easy to use  
 affordable solution!




**Schneider**  
 GEOSPATIAL

# Putting you first - in everything we do.

At Community State Bank, we're all in when it comes to helping you and the greater Des Moines community thrive. That's why we put employees, customers and communities first – in everything we do.

Find out how CSB will put you first.







**IPAIT**  
IOWA PUBLIC AGENCY INVESTMENT TRUST

## The IPAIT Advantage

Comprehensive Investment Solutions  
designed for Safety, Liquidity and Yield

IPAIT Board Representatives:  
 Craig Anderson - Plymouth County Supervisor    Jarret Heil - Marshall County Treasurer    Dan Zomermaand - Sioux County Treasurer

Contact Paul Kruse: (515) 554-1555 | toll-free (800) 269-2363 | pkruse@pmanetwork.com

Sponsors:





Investment Advisor/  
Administrator/Marketer:



©2020 PMA Securities, LLC. All rights reserved. Visit [www.ipait.org](http://www.ipait.org)



## Financing Solutions for Municipal Infrastructure

### Project Finance: Planning Through Maturity

Capital Planning

➤

Bond Issuance

➤

Post-Sale Compliance

### Full Service Platform:

- Placement Agent
- Underwriter
- Municipal Advisory

**Scott Stevenson**, Managing Director  
(515) 471-2721 | [SStevenson@dadco.com](mailto:SStevenson@dadco.com)

**Michael Maloney**, Senior Vice President  
(515) 471-2723 | [MMaloney@dadco.com](mailto:MMaloney@dadco.com)

**Nathan Summers**, Vice President  
(515) 471-2722 | [NSummers@dadco.com](mailto:NSummers@dadco.com)



**D | A | DAVIDSON**  
FIXED INCOME CAPITAL MARKETS  
D.A. Davidson & Co. member SIPC and FINRA

515 East Locust St., Suite 200 | Des Moines, IA | (515) 471-2700 | (800) 642-5082 | [dadavidson.com](http://dadavidson.com)





6903 Vista Drive  
West Des Moines, IA 50266  
[www.northlandsecurities.com](http://www.northlandsecurities.com)  
515-657-4675  
Member FINRA and SIPC  
Registered with SEC and MSRB



- *Competitive Bond Sales*
- *Debt Refinancing*
- *Property Tax Impact Analysis*
- *Tax Increment Financing*
- *Financial Management Plans*
- *Bond Underwriting*
- *Continuing Disclosure*
- *Bank Private Placement*
- *Referendum Assistance*
- *Capital Improvement Plans*
- *Equipment Financing*

### NORTHLAND'S IOWA TEAM

- *Commitment to integrity*
- *Creative solutions to complex issues*
- *Engaged team approach*
- *Customized financial planning models*
- *Staff with depth and experience*



**Heidi Kuhl**  
Director  
[hkuhl@northlandsecurities.com](mailto:hkuhl@northlandsecurities.com)  
515-657-4684

**Jeff Heil**  
Managing Director  
[jheil@northlandsecurities.com](mailto:jheil@northlandsecurities.com)  
641-750-5720



**Chip Schultz**  
Managing Director  
[cschultz@northlandsecurities.com](mailto:cschultz@northlandsecurities.com)  
515-657-4688




RC 20-403; Muni 20-274 10/20

Henry M. Adkins and Son, Inc. (Adkins) was founded in 1939 by Henry Merritt Adkins and has maintained representation in the county government field for over 75 years. In 2011, Adkins became a business partner with Unisyn Voting Solutions, selling and supporting Unisyn voting system products. Our staff has over 100 years of experience in conducting elections and providing quality products and exemplary service to our clients.



- **Full Service Election Provider**
- **Unisyn Voting Solutions voting equipment**
- **Tenex Electronic Poll Books**
- **Tenex Election Night Reporting**
- **EasyVote Election Management Software**



**Summit Carbon Solutions is proud to partner with ethanol plants across Iowa to make the industry more competitive and profitable for decades to come.**

- Summit Carbon Solutions will help its ethanol plant partners **lower their carbon emissions and compete in fuel markets across the country.**
- Opening these new marketplaces will **maintain strong land values and commodity prices**, while **improving the long-term economic outlook** for ethanol producers and Iowa landowners.
- This project will **support local businesses, suppliers, and workers** to provide a meaningful, ongoing boost to the economy of local communities.
- Summit Carbon Solutions will create **thousands of high-quality jobs** during construction and **hundreds of full-time jobs** once operational.

## Our Partners

Corn LP – Goldfield (IA)  
Golden Grain Energy – Mason City (IA)  
Green Plains, Inc. – Shenandoah (IA)  
Green Plains, Inc. – Superior (IA)  
Homeland Energy Solutions – Lawler (IA)  
Lincolnway Energy – Nevada (IA)  
Little Sioux Corn Processors – Marcus (IA)  
Louis Dreyfus – Grand Junction (IA)  
Pine Lake Processors – Steamboat Rock (IA)  
Plymouth Energy – Merrill (IA)  
Quad County Corn Processors – Galva (IA)  
Siouxland Energy Cooperative – Sioux Center (IA)

To learn more, visit [www.SummitCarbonSolutions.com](http://www.SummitCarbonSolutions.com).



**SUMMIT  
CARBON  
SOLUTIONS**

# ISAC GROUP BENEFITS PROGRAM

PARTNERING WITH COUNTIES ACROSS IOWA



## Health Program

- Early release of renewal rates
- Experience and wellness discounts
- Multiple networks and plan designs
- 28 participating counties



## Worksite & Ancillary Program

- Group accident and critical illness plans
- Accident includes wellness benefit
- Voluntary Life and Voluntary AD&D
- Group disability products



## Dental Program

- Comprehensive plan portfolio
- Voluntary and contributory pricing
- Broad network of providers
- 29 participating counties



## Complimentary ISAC Benefits

- Wellness Program
- Employee Assistance Program
- COBRA administration
- Consolidated Billing



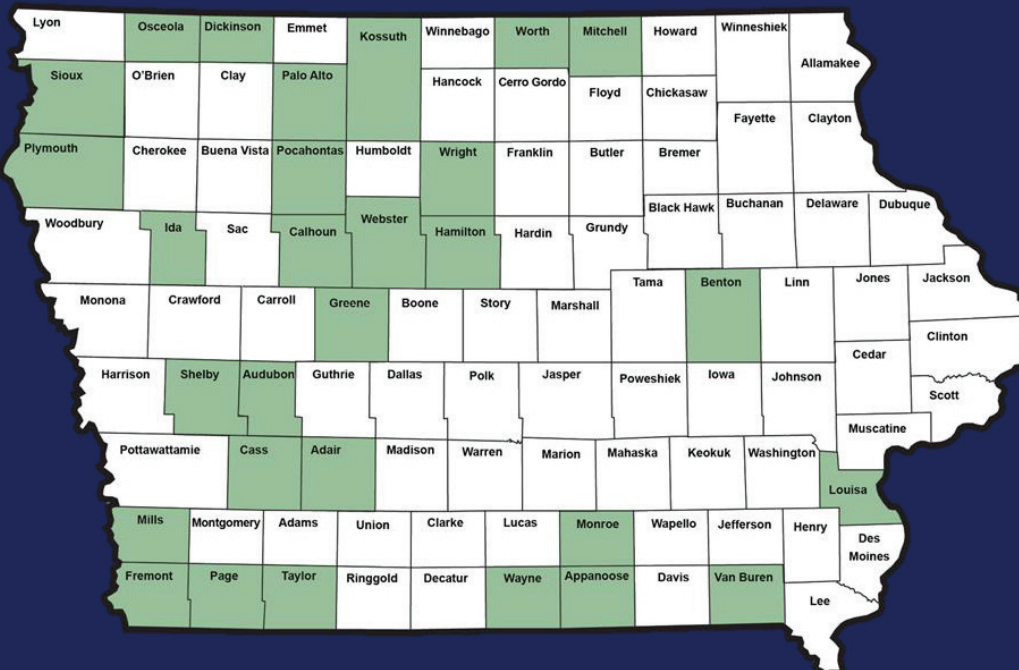
## Vision Program

- Multiple carriers and plan options
- Exclusive fully insured county pricing
- Robust provider networks
- 23 participating counties



## AssuredPartners

- Employee benefits consulting
- Dedicated service team
- Compliance assistance
- Online enrollment platform



Current Members

**ISAC**  
Iowa State Association of Counties

**AssuredPartners**

515-493-0802 | [assuredpartners.com](http://assuredpartners.com)





It might be CORNY, but it is no TRICK...

## COVERAGE DESIGNED SPECIFICALLY FOR COUNTIES IN IOWA.



Governing boards comprised of County Officials.



Coverage to meet the needs of Iowa communities.



Created to exclusively serve local governments in Iowa.

### COUNTY RISK MANAGEMENT SERVICES, INC.

*representing*



Providing property, casualty & workers' compensation for counties in Iowa.

Programs endorsed by ISAC | [crmsia.com](http://crmsia.com) | [icapiowa.com](http://icapiowa.com) | [imwca.org](http://imwca.org)