

# 2019 MMTA Fall Conference

*People. Purpose. Passion. The Flights of Success*

**Tues., Oct. 15, 2019 – 8:30 am: Ethics and Politics in the Workforce**



**Jeffrey G. Collins, Attorney-at-Law**

Jeffrey G. Collins is a native Detroit and honor graduate of Howard University School of Law. Jeffrey G. Collins has a distinguished 34-year legal career in both the public and private sector. He is a former judge of the Michigan Court of Appeals and Wayne County Circuit Court. Following the tragic events of 9/11, Jeffrey received a Presidential appointment to serve as the United States Attorney for the Eastern District of Michigan. In addition, he recently served as Deputy Wayne County Executive where he drafted an ethics policy for the executive department of Wayne County government.

Mr. Collins is currently the founding and managing partner of Collins & Collins, P.C. In 2014, he authored his first book, entitled, "Do the Right Thing: Make Ethics Your Brand." Mr. Collins has also served as an adjunct faculty member at Wayne State Law School, University of Michigan-Dearborn and Wayne County Community College. He has been recognized as a Michigan Lawyer of the Year and a Michigan Super Lawyer.

He has conducted numerous workshops on Ethical Leadership to corporate, governmental and educational organizations.

**2019 MMTA FALL CONFERENCE**  
**“ETHICS AND POLITICS IN THE WORKFORCE”**  
**HANDOUT MATERIALS**  
**ATTORNEY JEFFREY G. COLLINS**

1. The Treasurer is up for re-election. During the work day you are asked to speak at a community event about a new tax foreclosure program offered by the Treasurer. The Treasurer asks you to pass out his campaign literature after the meeting. You explain that this violates the county’s ethics ordinance. The Treasurer responds by saying the ethics ordinance is rarely enforced. He insists that you pass out his literature. What do you do?
  
2. The CEO of an organization had a favorite among her direct reports, a guy who was highly innovative and worked extremely hard. His peers, however, viewed him as the “teacher’s pet”. They kept him out of informal discussions, did not invite him to meetings and often ganged up on him when he presented a concept. In the CEO’s presence, they seemed to treat this teacher’s pet like everyone else. In private, however, they schemed against him in small but significant ways. What should the “teacher’s pet” do?
  
3. Your department has access to a suite at Ford Field for Detroit Lion football games. There are 25 people in your department. The suite holds only 5 people and your department has been given the suite for 4 games. Elected officials, vendors, community supporters and managers of other departments have all been hounding your boss for tickets. Many are asking if they can bring a guest. Your boss asks you to develop a plan on how tickets will be distributed. What does your plan look like?

# 2019 MMTA Fall Conference

*People. Purpose. Passion. The Flights of Success*

**Tues., Oct. 15, 2019 – 9:45 am: Succession Planning**



**Mr. Brian J. Camiller, CPA, Plante Moran**  
**248.223.3840; [Brian.Camiller@plantemoran.com](mailto:Brian.Camiller@plantemoran.com)**

Brian is a partner with Plante Moran and has more than 21 years of experience working with governmental organizations, including counties, cities, townships, villages, libraries, retirement systems, and authorities. As the industry leader for Plante Moran Governmental Accounting Professionals (PMGAP), he oversees a team of 20 accountants and serves 50-60 governmental organizations per year. In addition to preparing organizations for the annual audit, creating municipal budgets and water and sewer utility rate models, and designing new chart of accounts, his team recently created a financial health assessment tool for economically troubled governments. He is a frequent presenter for municipal organizations, including MMTA. When not performing government accounting miracles, Brian enjoys coaching his kids' baseball and flag football teams.



**Christopher Gilbert, CPA, Plante Moran**  
**810.766.6008; [Christopher.Gilbert@plantemoran.com](mailto:Christopher.Gilbert@plantemoran.com)**

Chris is an audit manager with over five years of experience providing audit and assurance services to Plante Moran's governmental clients, primarily local units of government. He works on audit engagements including those with single audits and financial statements that are submitted to the GFOA's Certificate of Achievement for Excellence in Financial Reporting program. He has assisted multiple governmental entities with planning and implementation for GASB statements 67, 68, 74, and 75, among others. When not working on governmental audits, Chris enjoys participating in recreational basketball and flag football leagues and spending time with friends and family.

A hand is shown on the left side of the frame, holding a chain of white paper figures that resemble a paper chain. The figures are connected by their arms, forming a continuous line that stretches across the width of the image. The background is a solid dark blue color.

- {Succession Planning}

- Developing Your Next Generation of Leaders

plante  
*m*  
moran

audit • tax • consulting

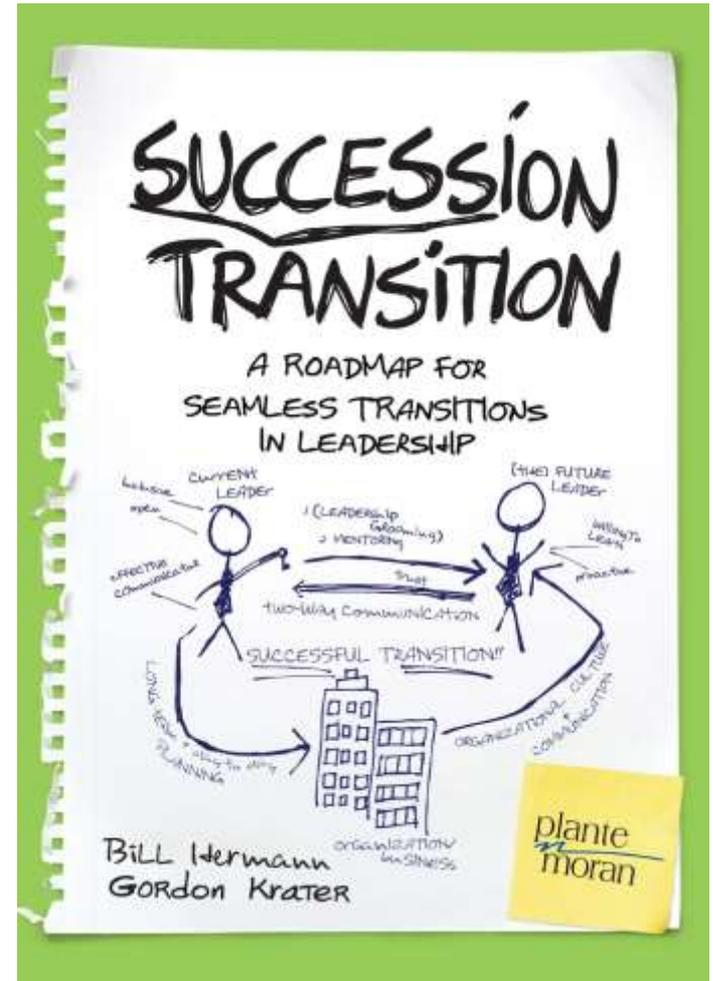
*Michigan Municipal Treasurers Association  
2019 Fall Conference*

# Agenda

- Why (When) Do Talent Initiatives Get Attention
- Creating the Business Case for Succession
- Creating a Talent Advantage: Multiple People & Multiple Roles
- Developing Your Next Generation of Leaders
- Re-recruiting
- Succession Planning Best Practices

# What Is Succession Planning?

- A process that ensures that the right people for the right positions are in place today, tomorrow, and 10 years from now
- Incorporates best practices concerning recruiting, development, and retention



# The Catalysts

- Why do talent initiatives get attention?



Planning for Success

Risk Mitigation

- The leader at the top is a believer in talent development.
- Key stakeholders see the business case for succession.
- There is a belief that bad things can happen if we don't do anything.

# Talent Initiatives Get Attention when...

- Organizations perform significantly below expectations
- Strategic opportunities arise
- Economical setbacks
- Key staff leave unexpectedly (Too late!)

# Creating a Business Case

- The Importance of Culture “Fit”
- The High Cost of Turnover
- INCREASING Diversity in the Work Place

# Importance of Culture Fit

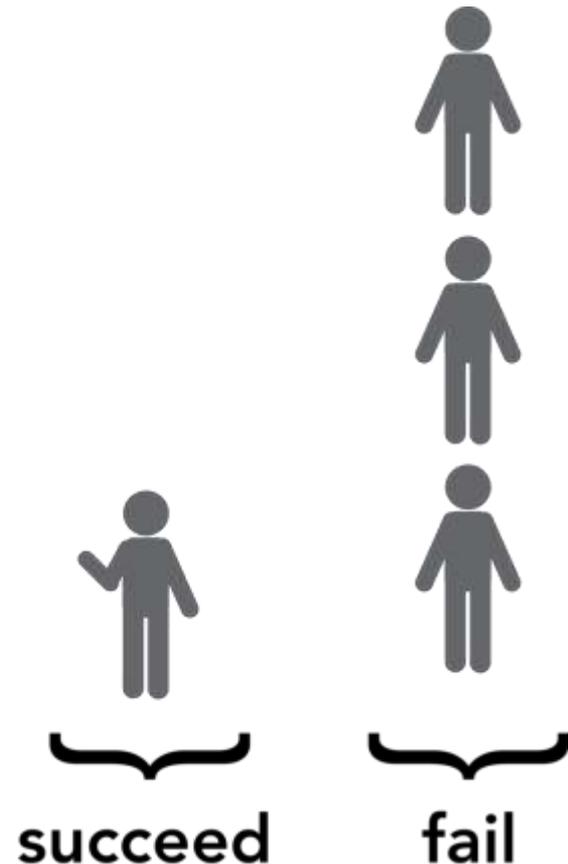
New managers and executives are

**3** times more  
likely to fail

because of not fitting with the

**culture**

and their peers rather  
than because of not  
having the skills.



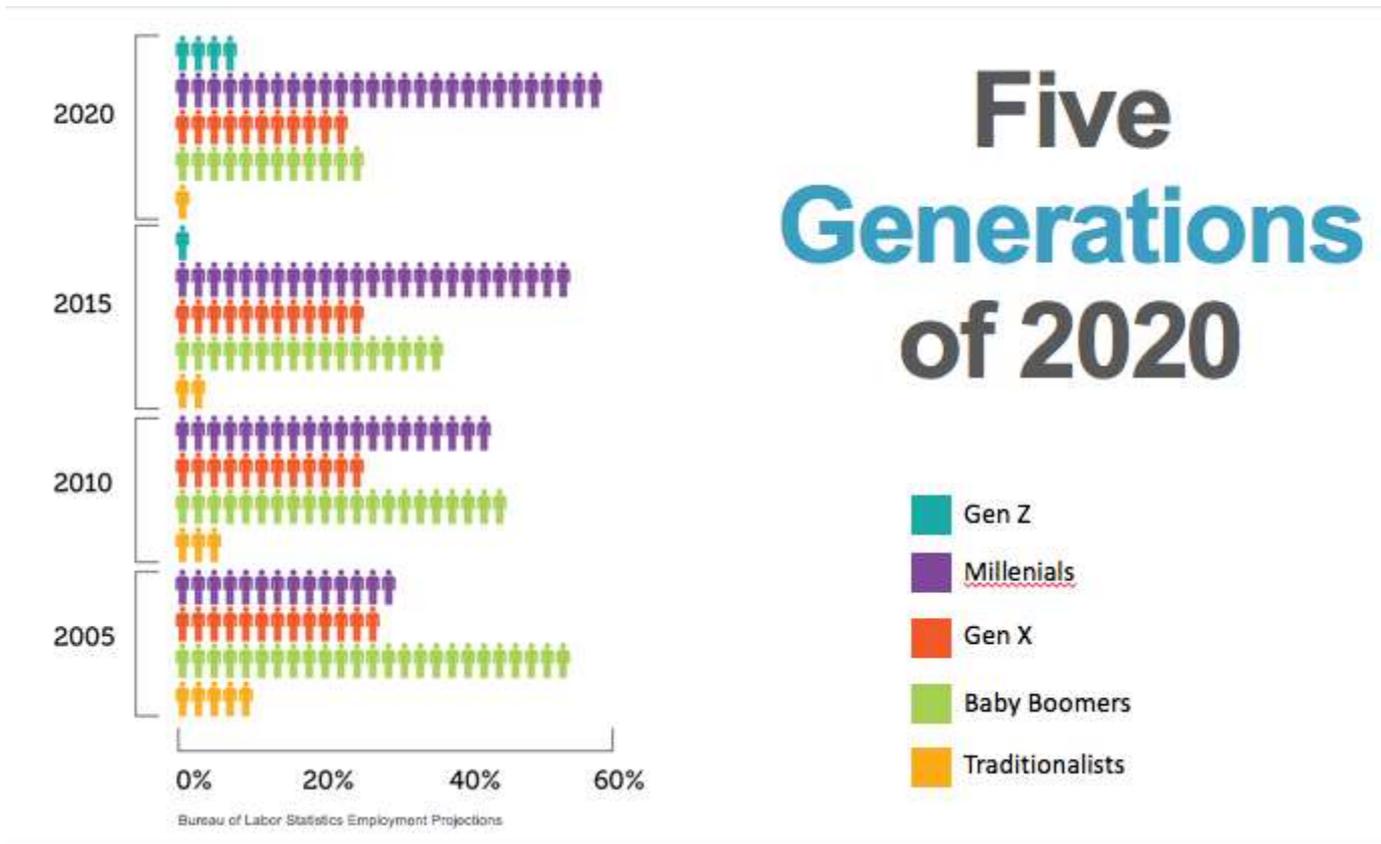
# The High Cost of Turnover

**cost**  
of a wrong hire

- \$75,000 position could cost an organization \$90,000 plus the added stress, cultural impact, and more...

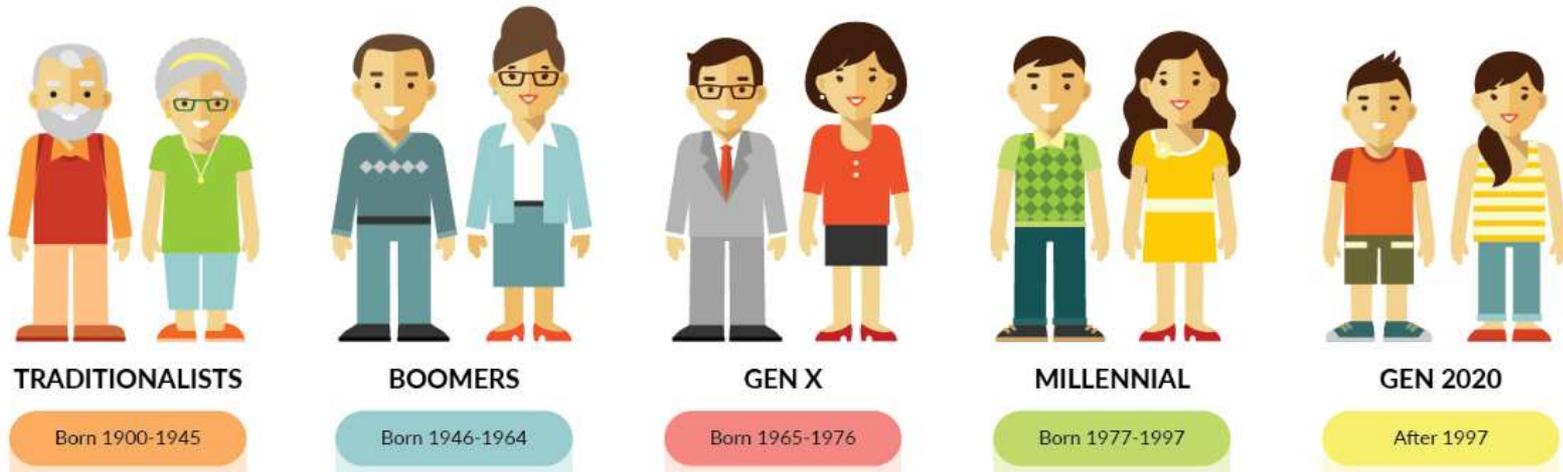


# Connecting Generations in the Workplace



# Generational Differences

## Five Generations Working Side by Side in 2020



- For the first time in history, five generations will be working side by side in 2020. Different values, experiences, styles, and activities create misunderstandings and frustrations
- Today, 70 million Baby Boomer will be eligible for retirement in large numbers
- Generation X, a generation with different sensibilities and priorities than Boomers, will assume positions of leadership in schools and districts

# Generational Differences

The Baby Boomers Thought Nothing of Getting Up at 5 a.m. to Work - The Younger Generation Doesn't Think Much of it Either.

Jack Welch

# Traditionalists

Traditionalist

1900-1945

## Societal Influences

- Great Depression
- Roaring 20s
- WWI & WWII
- Korean War
- GI Bill

## Characteristics

- Patriotic – Waste Not Want Not
- Faith in Institutions
- Military Influence
- Authoritarian leadership style
- Don't complain – Just Deal with it

## KEY WORDS: LOYALTY & LEGACY



When Generations Collide: Who They Are. Why They Clash. How to Solve the Generational Puzzle at Work”  
Lynne Lancaster and David Stillman

# Boomers

Boomer

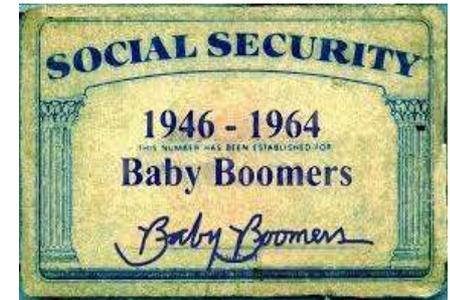
1946 - 1964

## Societal Influences

- Suburbia
- TV
- Vietnam
- Human Rights
- Music and Libations

## Characteristics

- Idealistic
- Competitive
- Not easily led – Question Authority



## KEY WORD: OPTIMIST

When Generations Collide: Who They Are. Why They Clash. How to Solve the Generational Puzzle at Work”  
Lynne Lancaster and David Stillman

# Gen X

Gen X

1965 - 1976

## Societal Influences

- Sesame Street
- MTV
- Game Boy
- PC
- Divorce Rate Tripled
- Latch Key Children

## Characteristics

- Eclectic
- Resourceful
- Self-reliant
- Distrustful of institutions
- Highly Adaptive to Change and Technology



## KEY WORDS: SKEPTICISM

When Generations Collide: Who They Are. Why They Clash. How to Solve the Generational Puzzle at Work”  
Lynne Lancaster and David Stillman

# Millennial – Gen Y

Millennial

1977 - 1997

## Societal Influences

- Expanded technology
- Natural disasters
- Identity theft
- Terrorism

## Characteristics

- Globally connected
- Cyber literate
- Personal safety is primary concern
- Mobile device functions as 5<sup>th</sup> limb



## KEY WORD: ACCESS

When Generations Collide: Who They Are. Why They Clash. How to Solve the Generational Puzzle at Work”  
Lynne Lancaster and David Stillman

# Gen Z (2020)

Gen Z

After 1997

## Societal Influences

- Social Media
- Technology
- Their own peers
- Individual expression
- The Great Recession

## Characteristics

- Multi-tasking
- Entrepreneurial
- High Expectations
- Finds fulfillment in their Devices (Phones, Tablets)
- Prefer cool products over cool experiences



## KEY WORD: Unique & Realistic

When Generations Collide: Who They Are. Why They Clash. How to Solve the Generational Puzzle at Work”  
Lynne Lancaster and David Stillman  
McKinsey&Company

# Creating a Talent Advantage: Multiple People, Multiple Roles

- As organizational challenges become increasingly complex, multiple leaders are needed to be successful.
- Top talent values career progression and challenge.
- Increasing emphasis on “successor planning,” planning to provide talent to meet future challenges and leadership roles.

# Developing Your Next Generation of Leaders



# Seven Suggestions to Create Next Generation Leaders

# 1. Create the Vision

What does a next generation leader in your organization look like?

- Build a model – define key success factors, skills, and competencies
- Develop a behavioral continuum

## 2. Get Real

How do you create meaningful, two-way dialogue focused on future development?

- Staff and Supervisor complete independent ratings of key factors, characteristics, and competencies
- Remember the person behind the ratings
- Focus the conversation on future development activities instead of past performance
- Separate development conversations from performance reviews

# 3. Leverage Strengths

Which strengths will be most helpful in becoming a successful next generation leader?

- It's not just about what a person is good at. Which of their skills will promote organizational success?
- Focus on no more than 3 “signature strengths”
- These skills take on greater and greater importance as a person moves up in the organization: the ability to implement strategy, influence others, build consensus, manage conflict, coach and develop staff, explore alternative perspectives with an open mind, improvise, and an effective executive presence.

## 4. Prioritize

What does it take to get to the next level?

- Focus on what the staff needs to do or become, not on the person's weaknesses or limitations
  - This creates a collaborative, problem-solving mindset and discussion
- Avoid a laundry list of improvement areas that fail to prioritize the most important issues to address

## 5. Stretch

# What assignments and activities make a difference?

- Stretch assignments help future leaders build skills, increase engagement, and promote a sense of contribution to the organization
- Upfront, explain the desired skills and outcomes
- Discuss how progress and success will be measured at the end
- Afterwards, debrief key learnings and how to apply lessons learned

## 6. Coach & Sponsor

What can the supervisor/  
mentor do to support growth?

- Give stretch assignments
- Make introductions, advocate for additional assignments, provide context for how individual development plans fit with career progression
- Timely, specific, and balanced performance feedback
- Ongoing encouragement and coaching
- Candor is kindness

## 7. Nurture a Growth Mindset

How do you create an ongoing conversation focused on learning rather than default to an annual event focused on past performance?

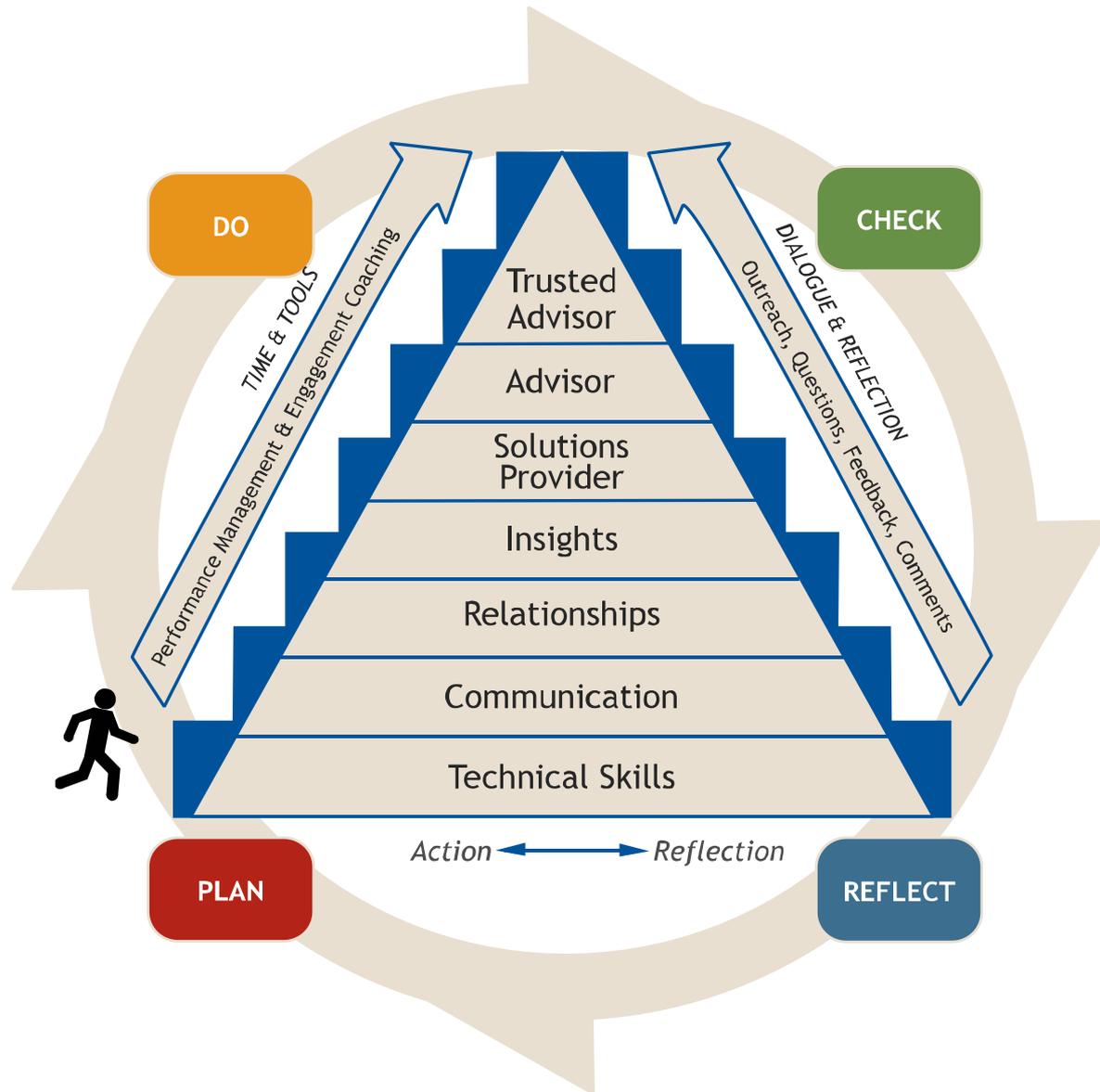
- Foster a “growth mindset” – everyone can grow and improve their skills and abilities in specific areas
- Ability to learn from experience and apply this learning to future challenges is a differentiating factor between next-gen leaders
- Integrate development discussions into check-in meetings
  - Don't let the development plan sit on the shelf; it is a living, breathing document

# Learning: Pyramid of Progress

- A comprehensive method of performance development and assessment for all managers and staff.
- Composed of competencies, personal qualities, results measures, and overall goals.
- Functions as an individualized roadmap for each person across each department in the government.

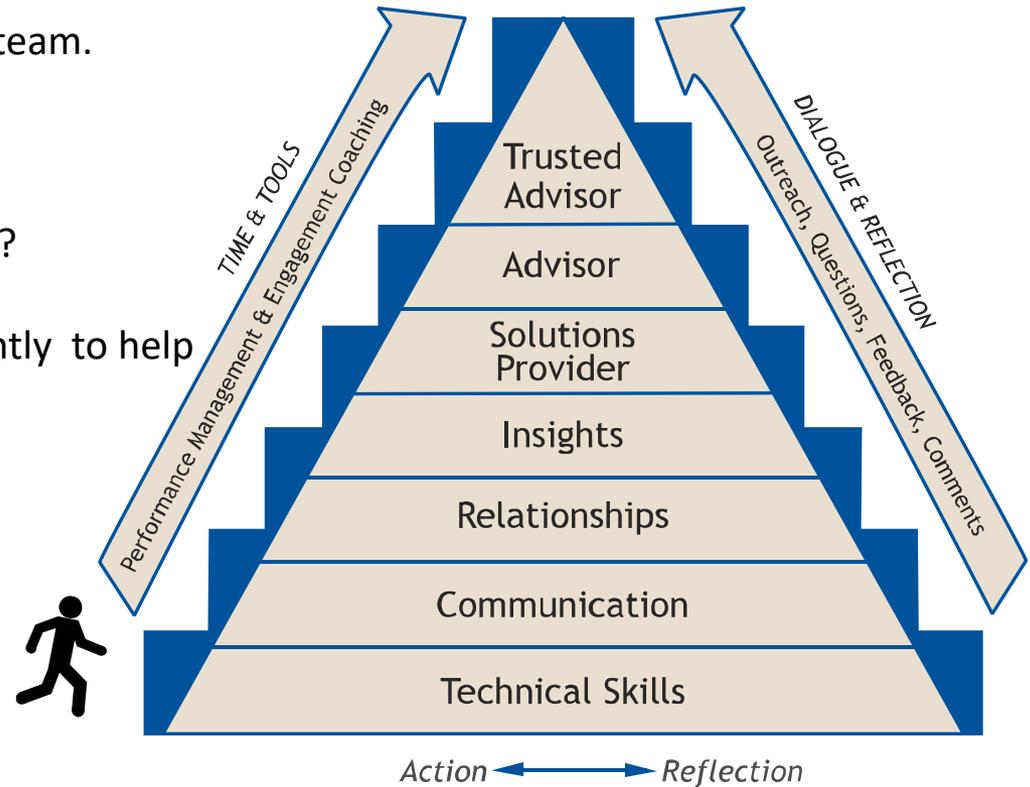


# Pyramid of Progress

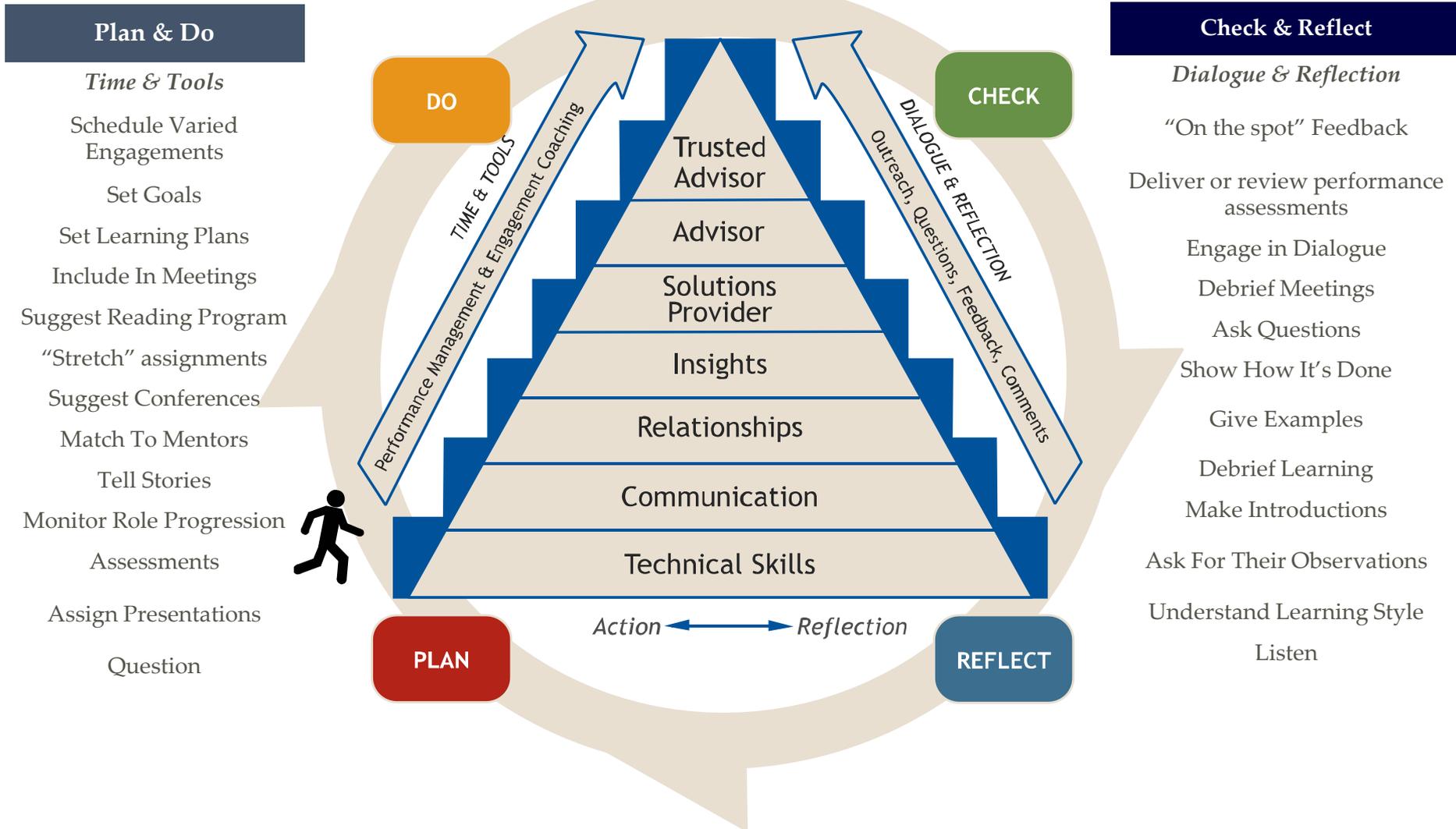


# Pyramid of Progress: Activity

1. Think about a direct report on your team.
2. Where are they on the pyramid?
3. What skills do they need to advance?
4. What can you as a leader do differently to help them advance to the next level?



# Pyramid of Progress



But sometimes, despite your efforts, the talent you worked so hard to develop, decides to seek greener pastures.

# Re-Recruiting

- Developing and maintaining a close relationship with key staff.
- Spending quality time with staff.
- Knowing the answer to the question: “Why do staff members work for your organization rather than another organization?”
- “Know what you might do if a valued staff member said he or she was leaving – and then do it now”.

\* Reference: Succession Transition: A roadmap for seamless transitions in leadership. (2011) Bill Hermann & Gordon Krater

# Re-Recruiting

- “... invest a little extra time in making them (staff) feel wanted and appreciated, as if you were attempting to bring them on board for the first time.”
  - Pause and take note of your top performers.
  - Take a moment to thank them.
  - Spend time with them.
  - Offer professional development opportunities for them.
- *Reference: Re-Recruiting: Your best defense against restless feet. Holly Green. Forbes.com, 5/13/11*

# Best Practices in Succession Planning

- Incorporate succession planning and talent development into your strategic plan.
- Link leadership competencies to organizational challenges.
- Focus on broad range of key positions, not just the top leader.
- View the plan as a roadmap to be updated: not a one-time event.
- Create individual talent action plans that align with key organizational goals and objectives
- Provide challenge and stretch assignment(s) for top talent

Thank you.

**Brian Camiller**

248.223.3840

brian.camiller@plantemoran.com

**Chris Gilbert**

248.766.6008

christopher.gilbert@plantemoran.com

# 2019 MMTA Fall Conference

*People. Purpose. Passion. The Flights of Success*

**Tues., Oct. 15, 2019 – 11:00 am: Homeland Security Assessment Services for Municipalities and**  
**Tues., Oct. 15, 2019 – 1:00 pm: Cyber Threats and How to Protect Yourself**



**Kelley Goldblatt, Cybersecurity Advisor, U.S. Department of Homeland Security**  
**202-893-2304; [kelley.goldblatt@hq.dhs.gov](mailto:kelley.goldblatt@hq.dhs.gov)**

Kelley Goldblatt is the Cybersecurity Advisor for Michigan and Ohio with the Cybersecurity and Infrastructure Security Agency (CISA). In this role, Ms. Goldblatt supports the mission of strengthening the cyber resilience and security of the nation's critical infrastructure. Prior to joining CISA, Ms. Goldblatt worked in positions which helped Michigan organizations and residents become more cybersecure.

## Origin Story

CISA evolved out of the Department of Homeland Security's legacy National Protection and Programs Directorate (NPPD). Many of the strong partnerships with public sector, private sector, and government partners that NPPD developed drove the changes that culminated in the creation of CISA.

The original mission has evolved along with the dynamic threat environment, which today runs the gamut from protecting federal networks to protecting soft targets and crowded places. To meet our stakeholders' maturing needs and capabilities, CISA took the place of NPPD as an operational agency with its own authorities under the DHS umbrella.

As an agency with its own authorities, CISA can better align physical infrastructure and cybersecurity efforts, streamline partner engagements, and more clearly define product and service offerings. The result? A more effective approach to the threats we face today and tomorrow.

## Three Principles Drive Our Mission



**Partnership & Collaboration.** No agency, government, or business can singularly manage the complex risks that face us today. Simply put, we are more effective together than we are on our own.



**Sharing Information.** Federal, state, local, tribal, territorial, and private sector partners need to share accurate information—quickly—to ensure our critical infrastructure is secure.



**Transparency.** CISA will be transparent about the threat, and about the things we are doing with our partners to counter that threat.

## CONNECT WITH US

[cisa.gov](https://cisa.gov)



**CISA**  
CYBER+INFRASTRUCTURE

### Report Incidents, Phishing, Malware, or Vulnerabilities

(888) 282-0870 | [info@us-cert.gov](mailto:info@us-cert.gov)  
[us-cert.gov/report](https://us-cert.gov/report)

### National Cybersecurity & Communications Integration Center (NCCIC) Resources

(888) 282-0870 | [ncciccustomerservice@hq.dhs.gov](mailto:ncciccustomerservice@hq.dhs.gov)



Twitter

[@cisagov](https://twitter.com/cisagov) | [@cyber](https://twitter.com/cyber) | [@uscert\\_gov](https://twitter.com/uscert_gov)



LinkedIn

[linkedin.com/company/cybersecurity-and-infrastructure-security-agency](https://linkedin.com/company/cybersecurity-and-infrastructure-security-agency)



# CISA

The Cybersecurity and Infrastructure Security Agency



**CISA**  
CYBER+INFRASTRUCTURE

U.S. Department of Homeland Security  
Cybersecurity and Infrastructure Security Agency



## DEFEND TODAY. SECURE TOMORROW.

Americans enjoy and expect reliable, secure, and efficient critical infrastructure. Most people can turn on the tap, take public transit, make a call, and place a financial transaction without wondering whether it will be safe or thinking about the technology working in the background to make these things happen.

We want it to stay that way, which is why Congress and the President created the Cybersecurity and Infrastructure Security Agency. CISA leads the Nation's efforts to understand and manage risk to our critical infrastructure from a constantly evolving range of cyber and physical threats.

### It's All Connected

Critical infrastructure is increasingly interdependent and connected. A threat to one part of this infrastructure can impact other sectors quickly. Through strategic partnerships, we can **Defend Today** and **Secure Tomorrow** against threats and risks to our infrastructure by leveraging each other's strengths.

By joining our unique capabilities, skills, and knowledge, industry and government can work together to keep America resilient and secure against cybersecurity and physical threats.

**CISA is at the center of this collective security effort.**

## Defending Today

As an agency within DHS, CISA's enduring mission is to lead the Nation's efforts to understand and manage risk to our critical infrastructure. CISA accomplishes this mission through the following key functions:

- **National Risk Management:** Risk is complex. CISA helps clear the clutter for solid decisions by providing context and guidance developed in partnership with industry. Current initiatives include:
  - Election security and resilience
  - Information and communication technology supply chain risk management
  - Cross-sector risk management planning and coordination
  - Pipeline cybersecurity
  - Electromagnetic pulse risk management
  - Position, navigation, and timing
  - Securing unmanned aircraft systems
  
- **Infrastructure and Cybersecurity Operations:** CISA coordinates infrastructure security and resilience efforts through trusted partnerships across the private and public sectors. CISA provides:
  - Vulnerability assessments
  - Alerts and notifications of elevated risk exposure
  - Training and technical assistance
  - Incident management operations
  - Consolidated all-hazards risk management for critical infrastructure
  - Chemical security regulatory enforcement
  
- **Critical Infrastructure Resilience:** CISA develops trusted partnerships across the private and public sectors to help critical infrastructure partners increase security and resilience through:
  - Information sharing
  - Advisory and planning assistance services
  - Training
  - Best practices, standards, and regulation development
  - Exercise design and facilitation
  - Evaluation
  - International critical infrastructure engagement



- **Federal Information Security:** CISA helps secure and boost federal civilian enterprise networks and the ".gov" domain resilience by providing:
  - Defensive technologies and monitoring capabilities
  - Cyber response operations
  - Capacity-building services for partner departments and agencies
  
- **Interoperable Emergency Communications:** CISA enhances and ensures effective public safety communication at all levels in the event of natural disasters, acts of terrorism, and other man-made disasters. CISA supports federal, state, local, tribal, territorial, and industry partners with:
  - Extensive outreach
  - Training
  - Coordination
  - Tools
  - Guidance
  - Technical assistance
  - Communications tools and access

## Securing Tomorrow: Meeting the Challenges Together

What lies over the horizon? The physical and cybersecurity landscape is constantly evolving. Predictions about the future range from the mundane to the unbelievable. As new technologies change the way we live and do business, new threats will emerge that require our collective attention. Bigger and more complex disasters will require quick, effective responses. And new solutions will drive our collective security.

**It's our mission—and our passion—to work with you, our industry and government partners, to keep America secure. No matter what the future brings.**



# CYBERSECURITY FOR SLTT GOVERNMENT

State, local, tribal, and territorial (SLTT) governments face daily cyberattacks and incidents as they serve customers and manage information online.

## DO YOU WORRY:

- How vulnerable is your business to cyberattack?
- How vulnerable is your network to cyberattack?
- Is your company doing all that it can to secure its network?
- How safe is customer and corporate information in your network?
- How would a cyberattack affect your business

You are not alone. We are here to help you. The **Cybersecurity and Infrastructure Security Agency (CISA)** is committed to helping the private sector manage cyber risk, reduce the frequency and impact of cyberattacks and incidents, and increase resiliency.

We help you by developing and promoting best practices, information sharing, and incident response to increase our Nation's cybersecurity. We're not law enforcement, we're not intelligence, and we're not regulators. Our sole job is to help you be more cyber secure.

## BEST PRACTICES

Adopting cybersecurity best practices is not a static, check-the-box compliance exercise but a continual use of evolving tools, services, and products to minimize risk and maximize security.

The **Cybersecurity Framework**, created jointly by industry and government, offers standards, guidelines, and best practices to help improve cybersecurity for any business. For more information, visit [nist.gov/cyberframework](https://www.nist.gov/cyberframework). To support its use, CISA offers free technical assistance, tools, and resources, such as risk assessments, to help manage cyber risk. For more information, visit [cisa.gov](https://www.cisa.gov).

**Risk assessments** are critical to understanding risk. CISA offers both self-assessments, taken independently by downloading evaluation forms from the CISA website, and on-site assessments by CISA cybersecurity experts. For more information, visit [cisa.gov](https://www.cisa.gov).

In many entities, control systems are managed separately from IT systems. CISA offers separate control systems assessments for businesses. For more information, visit [cisa.gov](https://www.cisa.gov).

## INFORMATION SHARING

Information sharing is integral as warnings of attacks, incidents, and network abnormalities can reduce the number of victims and lessen the impact. For more information, visit [www.dhs.gov/topic/cybersecurity-information-sharing](https://www.dhs.gov/topic/cybersecurity-information-sharing).

CISA understands the sensitivity of sharing cyberattack and incident information. Under the CISA **Protected Critical Infrastructure Information (PCII) Program**, your information is protected from public release when shared with CISA. For more information, visit [www.dhs.gov/how-pcii-protected](http://www.dhs.gov/how-pcii-protected).

CISA works closely with industry-specific **Information Sharing and Analysis Centers (ISACs)**. For more information, visit [www.isaccouncil.org](http://www.isaccouncil.org). For entities that may be in different industries but share a common interest and want to share information with one another, standards and guidance have been developed for the formation of **Information Sharing and Analysis Organizations (ISAOs)**. For more information, visit [www.dhs.gov/isao](http://www.dhs.gov/isao).

CISA offers free information that includes weekly bulletins, alerts on vulnerabilities and patches, detection information about emerging threats, and warnings and alerts through the **National Cyber Alert System**. For more information, visit [www.us-cert.gov/ncas](http://www.us-cert.gov/ncas). In the control systems arena, CISA shares specialized alerts and advisories along with reports and newsletters. For more information, visit [www.ice-cert.uc-cert.gov](http://www.ice-cert.uc-cert.gov).

CISA also offers an **Automated Indicator Sharing (AIS)** capability, a free, two-way information-sharing resource between government and private-sector participants that relays, at machine speed, signs of suspicious network activity that indicate threats. For more information, visit [www.us-cert.gov/ais](http://www.us-cert.gov/ais).

CISA's **Enhanced Cybersecurity Services (ECS) Program** helps protect public and private-sector entities from unauthorized network intrusions. CISA shares classified cyber threat indicators with qualified Commercial Service Providers that use the information to protect their customers. For more information, visit [www.dhs.gov/enhanced-cybersecurity-services](http://www.dhs.gov/enhanced-cybersecurity-services).

For companies that can collaborate, CISA offers the **Cyber Information Sharing and Collaboration Program (CISCP)**. CISA shares cyber threat, incident, and vulnerability information in near real time and works with partners to better understand threats and improve network defense. For more information, email [ciscp.coordination@hq.dhs.gov](mailto:ciscp.coordination@hq.dhs.gov).

---

## INCIDENT RESPONSE

Cyber incidents will occur if adversaries are determined. CISA is here to help. CISA's cyber response teams work with private and public-sector customers and international partners to respond to incidents. On request by the private sector, CISA can send fly-away teams to work on-site in response to incidents, including those on industrial control systems.

CISA includes in its incident arsenal such tools and services as the **National Cybersecurity Assessment and Technical Services (NCATS) Program**, which includes penetration testing, wireless discovery and identification, web application and scanning, and database and operating-system scanning. For more information, email [ncats\\_info@hq.dhs.gov](mailto:ncats_info@hq.dhs.gov).

Other incident response services include digital media and malware analysis, incident source identification, analysis of the extent of the compromise, recovery strategy development, and improved defenses. For more information or to request response services, email [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov).

---

## LINKS

To report a cyber incident, call 1-888-282-0870 or visit [cisa.gov](http://cisa.gov).

# 2019 MMTA Fall Conference

*People. Purpose. Passion. The Flights of Success*

**Tues., Oct. 15, 2019 – 2:15 pm: How to Control Access to Confidential Information**



**Sarah Jennings, CPA, CFE, CAE, Principal, Accounting and Outsourced Solutions, Director of Strategic Initiatives and Community Engagement, Maner Costerisan  
(517) 886-9502; [sjennin@manercpa.com](mailto:sjennin@manercpa.com)**

Sarah joined Maner Costerisan in 2003. She currently serves as a principal in the firm's Accounting and Outsourced Solutions department, leads Maner Costerisan's fraud and forensics practice and is a member of Maner Costerisan's nonprofit committee. Sarah oversees outsourced solutions engagements providing guidance and advisory services to client leadership and teams on financial analysis, projections and workflow. She has particular specialization performing fraud risk assessments and internal control process improvements for organizations across various industries. Sarah maintains a strong desire to help her clients augment their internal controls and fraud prevention systems, while minimizing their costs in the process. Sarah also performs examinations for various organizations and individuals to determine and document the extent of loss due to fraud.

Sarah is leading the firm's initiatives in innovation and community engagement involving many internal team members as well as community leaders and stakeholders. This increased focus is an exciting representation of Maner Costerisan's concentration on its corporate social responsibility. Beyond her client responsibilities at Maner Costerisan, Sarah regularly shares her expertise with colleagues and peers by speaking on industry related topics including fraud (risk areas, prevention and detection), financial oversight, board governance and ethics.

Sarah is a graduate of Illinois Wesleyan University. She is a member of the American Institute of Certified Public Accountants, Michigan Association of Certified Public Accountants, Association of Certified Fraud Examiners, Lansing Chapter of the Association of Certified Fraud Examiners, American Society of Association Executives, Michigan Society of Association Executives, McLaren Greater Lansing Healthcare Foundation, Board of Trustees Treasurer, ATHENA International, Board of Trustees Treasurer, and the ATHENA Women's Interest Network

Sarah volunteers her time with various charitable organizations primarily focused on leadership and entrepreneurship.



**Christopher S. Patterson, Member, Fahey Schultz Burzych Rhodes  
517.381.3205; [cpatterson@fsbrlaw.com](mailto:cpatterson@fsbrlaw.com)**

Christopher is a member at Fahey Schultz Burzych Rhodes PLC, where he focuses on the areas of municipal law, real property, and administrative law. Chris' expertise is highly regarded in his areas of practice, and he is frequently asked to present on hot topic issues at conferences and seminars across the state. Chris is identified as a Michigan Rising Stars Super Lawyer for 2019, current executive member and Past Chair of the Administrative Law Section of the State Bar, and co-chair of the Real Estate Section of the Ingham County Bar Association.

# **2019 MMTA Fall Conference**

*People. Purpose. Passion. The Flights of Success*

**Tues., Oct 15, 2019 – 3:30 pm: Treasurer to Treasurer: Relevant Issues Affecting Treasurers:  
Panel Discussion with Municipal Members**

**Townships:** Susan Daugherty, Treasurer, Green Oak Charter Township; Tim VanBennekom, Finance/Accounting Director/Deputy Treasurer, Allendale Charter Township; Bret Padgett, Treasurer, Comstock Charter Township

**Small Cities/Villages:** Rande Listerman, Clerk/Treasurer, Village of Pentwater; Travis Hewitt, Treasurer, City of Gaylord; Rachel Piner, Treasurer, City of Williamston; Ed Bradford, Finance Director/Treasurer, City of Manistee

**Large Cities/Villages/Counties:** Karen Coffman, Treasurer, Jackson County; Andrea Boot, Treasurer, City of Wyoming; Mary Ann Kornexl, Treasurer, City of Mt. Pleasant; Anthony Moggio, Finance Director/Treasurer, City of Rochester

