# State and Local Government Webcast Series

# Risks your government organization may not be considering

November 5, 2013

McGladrey

Assurance ▪ Tax ▪ Consulting

# Today’s presenters and agenda

**Patrick Hagan**
Partner
National State and Local Government Industry Leader
Chicago, IL

**Welcome**

**Sharon Griffin,** CFIRS, CRMA
Risk Advisory Services
Director
Los Angeles, CA

**Cash Controls**

**Corbin DelCarlo,** CISSP, QSA, PA-QSA
Security and Privacy Services Regional Leader
Chicago, IL

**PCI DSS Security**

McGladrey

# Today’s presenters and agenda (continued)

**Jermaine Stanley,** CISA
Public Sector National Practice
Manager
Vienna,  VA

**Cloud Computing Risks**

**John Croy**
Construction Risk Management National Leader
Phoenix, AZ

**Construction Contract Compliance**

McGladrey

# Cash control: A risk your organization may not be considering

Sharon Griffin, Risk Advisory Services Director

# Cash controls

- Misappropriation of funds (fraud or theft) can occur in any government agency handling cash
  - Transportation, utilities, courts, etc.

- Perpetrated by employees, vendors and even former employees

McGladrey

# Why have controls over cash items?

- Opportunities to commit fraud are likely to occur
  - When internal controls are weak
  - Where there's a lack of segregation of duties
  - When management has the ability to override preventative controls

- Cash has the greatest potential for theft if a system of internal controls is not in place and functioning effectively.

- Understanding how, when, and where cash is collected and the duties performed by each employee is imperative when designing the type of internal controls to implement.

- Although no system is foolproof, a well-designed set of internal control procedures can provide reasonable assurance that significant thefts of cash receipts and significant record-keeping errors will be prevented or detected.

*Source: Division of Local Government and School Accountability-Office of the State Comptroller*

# Cash collection procedures
## *(Think like a banker)*

- Limit the number of location sites (departments) – centralize cash collections
- Assign a separate cash drawer to each employee responsible for collecting cash
- Endorse checks immediately upon receipt
- Use sequentially numbered receipts and post notices for who to call if one is not provided
- Ensure deposits are balanced and verified under dual control and not tampered with
- Store cash in a secure facility or vault until it can be deposited
- Make deposits timely

McGladrey

# Internal controls

| Controls | Best practices |
|---|---|
| **Risk assessment and governance** | •Assess the risk of fraud or errors that can occur or go undetected entity wide<br>•Understand the control environment and determine what recourse or consequences should taken should cash be stolen<br>•Implement a whistleblower policy |
| **Policies and procedures** | • Finance or treasury department should have comprehensive cash handling policies and procedures to ensure cash items are received and deposited in a secure, timely and effective manner. |
| **Segregation of duties** | • Cash should be handled in dual-custody and no one person should have control over two or more steps in the process.<br>•Deposit slips should be signed and dated to evidence review and approval of the individuals preparing and verifying the deposit.<br>•Cash should be stored in dual controlled facility that restricts individual access |

McGladrey

# Internal controls

| Controls | Best practices |
|---|---|
| **Cash control** | •Cash handling procedures should be routinely audited to ensure they are being consistently followed |
| **Training** | • Provide cash handling training to departmental staff<br>• Where applicable, incorporate adherence to cash handling procedures as part of the staff's annual performance review so they are recognized for following policies and procedures, and that they are held accountable for misconduct. |
| **Physical security** | • For extra security, individuals handling cash should be seated in an area where there is camera coverage.<br><br>•To ensure that deposits cannot be tampered with once they are put into the safe, consider using tamper-proof bags or where practical, install an anchored in ground safe with drop slots. |

McGladrey

# PCI DSS security: A risk your organization may not be considering

Corbin DelCarlo, Security and Privacy Services Regional Leader

# Agenda

- What is PCI?
- What are my PCI obligations?
- Public sector PCI issues

McGladrey

# What is PCI?

- The PCI DSS was introduced to force the implementation of controls at service providers and merchants to protect CHD.
- The PCI DSS has very specific controls that can be implemented to reduce risk data compromise.
  - Based on 12 requirements
    - Roughly 235 sub-requirements which are specific controls to be implemented.
    - Designed with current breach methods in mind and focused on implementing controls that prevent data loss.


McGladrey

# What is PCI?

- Required for all organizations that store, process or transmit CHD
- Updated every three years
  - (3.0 in 2014)
- Compliance deadline for service providers was April 30, 2007
- Compliance deadline for all organizations was September 30, 2009
  - Why if the deadline past four years ago do so many organizations still not even know what PCI compliance is?
  - Compliance vs. validation


McGladrey

# What are my PCI obligations?

- Depends on merchant level
  - Levels 1 to 4 depending on transaction volume
    - More than 1 million transactions annually
      - Must do full assessment (via QSA or ISA)
    - Less than 1 million transactions
      - Can do self assessment questionnaire (SAQ)
    - Any transaction using a card with a VISA/Mastercard/Amex/Discover/JCB logo counts
      - Federal government prepaid VISA cards
        - Child support, unemployment, worker's comp, federal benefit payments, etc.
      - Automatic payments (ipass, taxes, payment plans)
- Always ask your acquirer what you have to do
  - Each acquirer is different
  - Acquirer is responsible for all their merchants

McGladrey

# Public sector PCI issues

- Most organizations typically need a year to become compliant
  - It varies depends on many things:
    - Priority of compliance
    - Number of gaps
    - Use of outside assistance

- However, most organizations only get 90 days to comply

McGladrey

# Public sector PCI issues

- Public sector organizations typically struggle with remediation efforts
  - First PCI assessment will always identify issues
  - Many of those issues will require funds to correct
    - FIM systems, AV, logging, policies, procedures, etc.

- Building in a budget for remediation at initial assessment can be critical to successful compliance

McGladrey

# Vendor management to reduce cloud computing risks

Jermaine Stanley, Public Sector National Practice Manager

# Agenda

- Cloud computing
- Top cloud security threats
- Vendor management to reduce risks

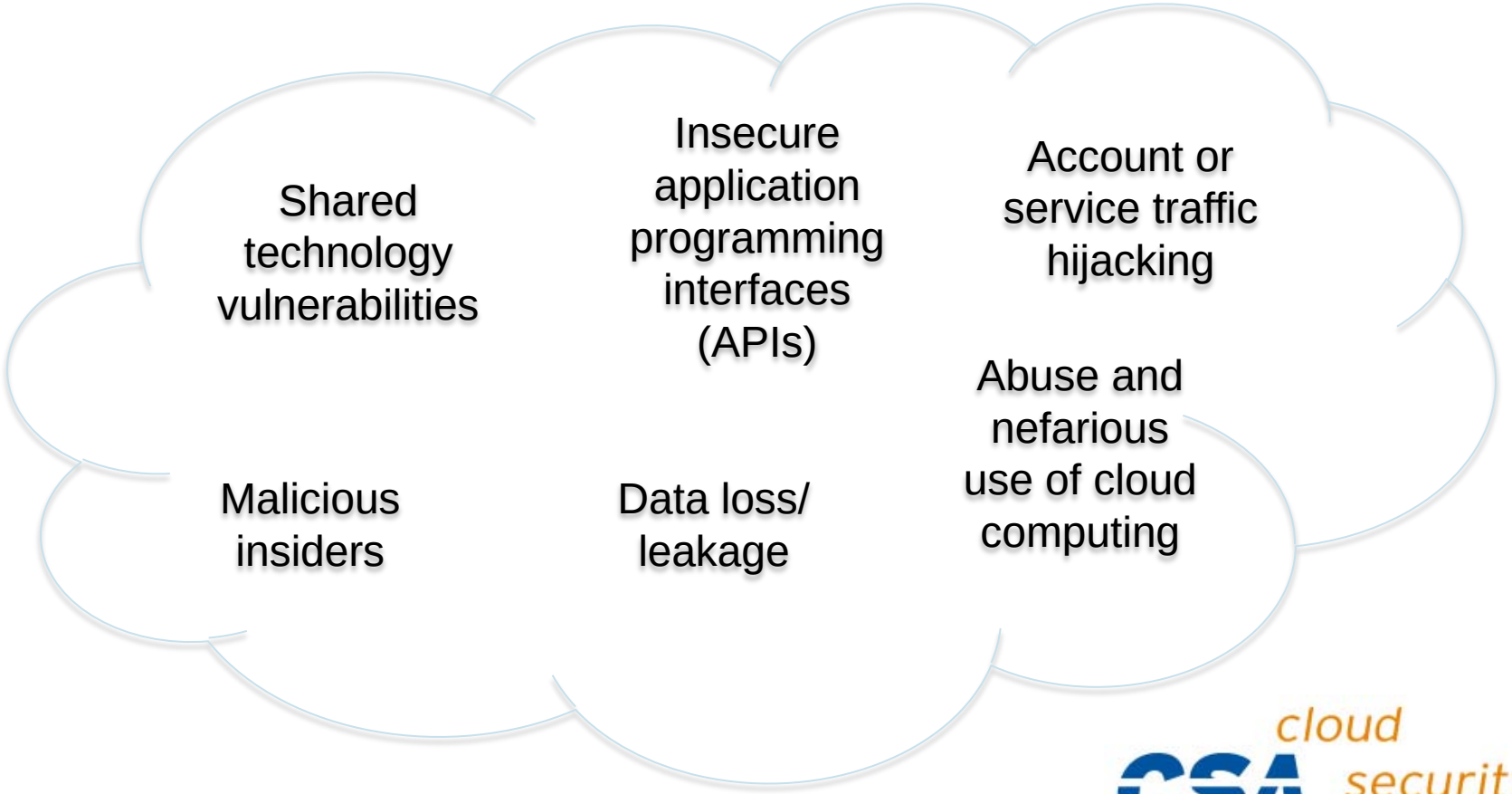
McGladrey

# A working definition of cloud computing

- A shared pool of configurable computing resources
  - convenient, on-demand
  - opportunity for management to reduce costs and respond to rapidly changing business needs
- Resources include – networks, servers, shared storage, applications, services
- NIST cloud model promotes availability and is composed of five essential **characteristics,** three **service models** and four **deployment models**.

McGladrey

# Top cloud security threats




cloud CSA security alliance

McGladrey

# Vendor management to reduce risk

- Vendor selection considerations
- Cloud vendor contract risks
- Managing vendor contract risks

McGladrey

# Vendor selection considerations

- Identify regulations and standards government entities are subject to
- Do vendors contractually hold themselves to the same regulations and standards?
  - For example:
    - Federal Information Security Management Act of 2002 (FISMA)
    - Organizations must meet the same security requirements that federal agencies require
    - NIST 800-53, revision 4
- Federal Risk and Authorization Management Program (FedRAMP)

*Source: Bank Systems and Technology*

McGladrey

# Cloud vendor contract risks

- Gartner Report
  - Most cloud computing contracts are more favorable to the vendor than to the customer
  - Often vague about how data will be protected
  - Don’t require meaningful compensation for the customer if a vendor mistake leads to data being compromised

- Negotiate with providers
  - The recent wave of cloud computing adoption is new
  - Customers have yet to negotiate for stronger security controls
  - 80% of organizations are unhappy with their vendor contracts*
  - Predicted that dissatisfaction will continue through 2015*

**Gartner Report*

McGladrey

# Managing vendor contract risks

- Audit and testing
- Security controls
- Compensation
- Data recovery
- Notification
- Exit strategies

*Source: IT Manager Daily: 6 Ways to Cloud Computing Contracts Put Security at Risk*

McGladrey

# Summary

- Cloud computing provides management with
  - An opportunity for reducing costs
  - Ability to react quickly to changing business needs
- Identify regulations government entities are subject to. *Do vendors hold themselves to the same regulations and standards?*
- Management should carefully look over vendor contracts and try to negotiate more favorable terms.
- While security/privacy issues are some of the biggest concerns for management, these can be effectively mitigated via sound vendor contract management.

McGladrey

# Construction Contract Compliance

John Croy, Construction Risk Management National Leader

# Agenda

- What determines risk
- Statistics
- Risk – stipulates sum projects
- Risk – cost reimbursable projects

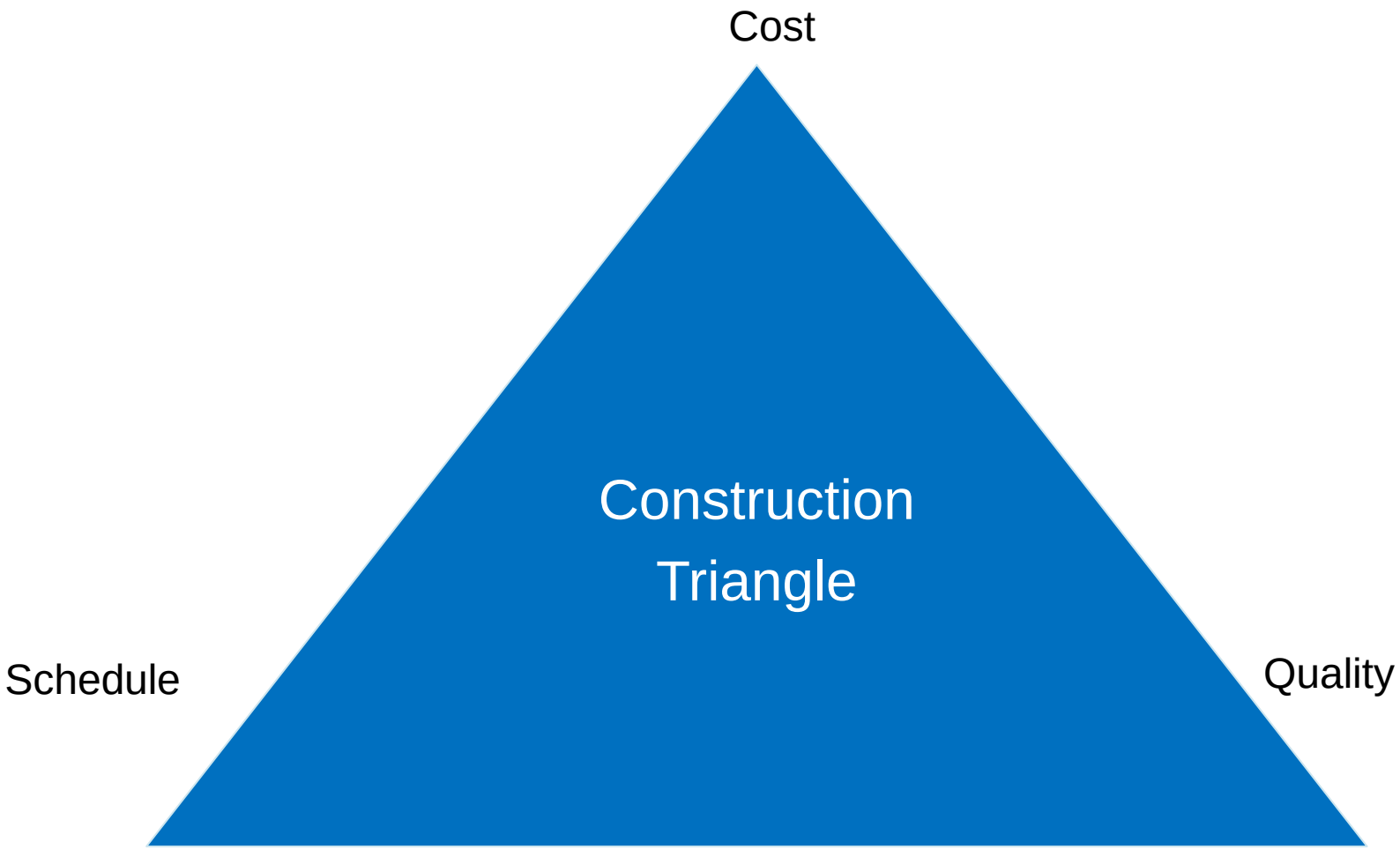
McGladrey

# Contract type determines risk

- Lump sum, fixed price, stipulated sum
  - Competitively bid
  - Negotiated
- Cost reimbursable or cost plus
  - Cost plus with fixed or percentage fee
  - Guaranteed maximum price
  - Time and material


McGladrey

# Construction risk




McGladrey

# Statistics

- ACFE statistics
  - Median fraud loss in construction is 300,000*
  - Third highest fraud loss amount by industry*
- ACFE common construction fraud schemes
  - Billings - 36%*
  - Corruption – 34%*

** Per The ACFE's 2012 Report To The Nations On Occupational Fraud and Abuse*

McGladrey

# Behavioral red flags

- Close association with vendors ($410,000)
- Wheeler dealer attitude ($405,000)
- Excessive pressure ($388,000)
- Control issues ($250,000)

** Per The ACFE's 2010 Report To The Nations On Occupational Fraud and Abuse*

McGladrey

# Stipulated sum – risks

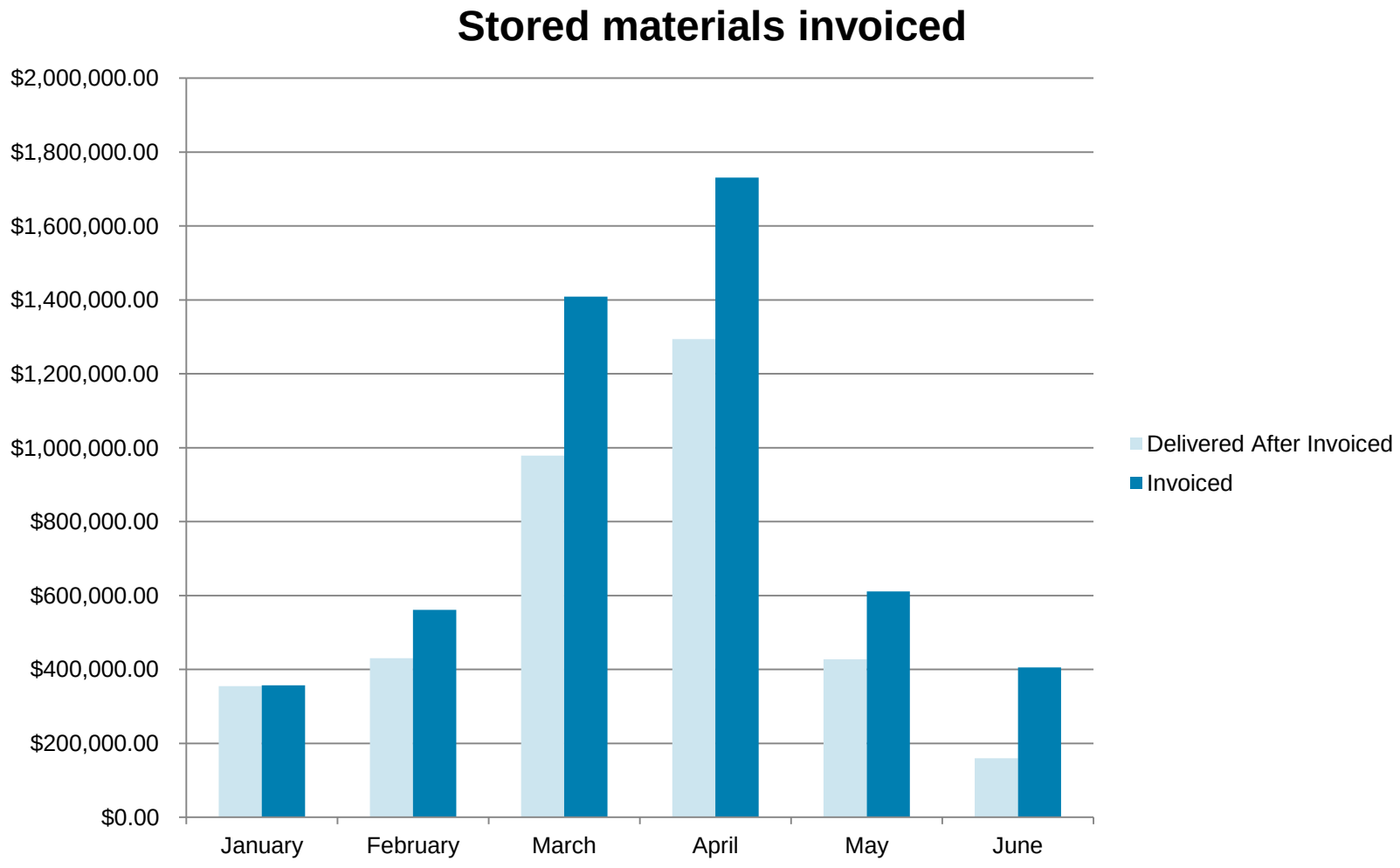
- Procurement process
- Specifications
- Change orders
- “Front-end” or “top-loading”
- Allowances
- Prevailing wage rates

McGladrey

# Change orders


McGladrey

# Stored material



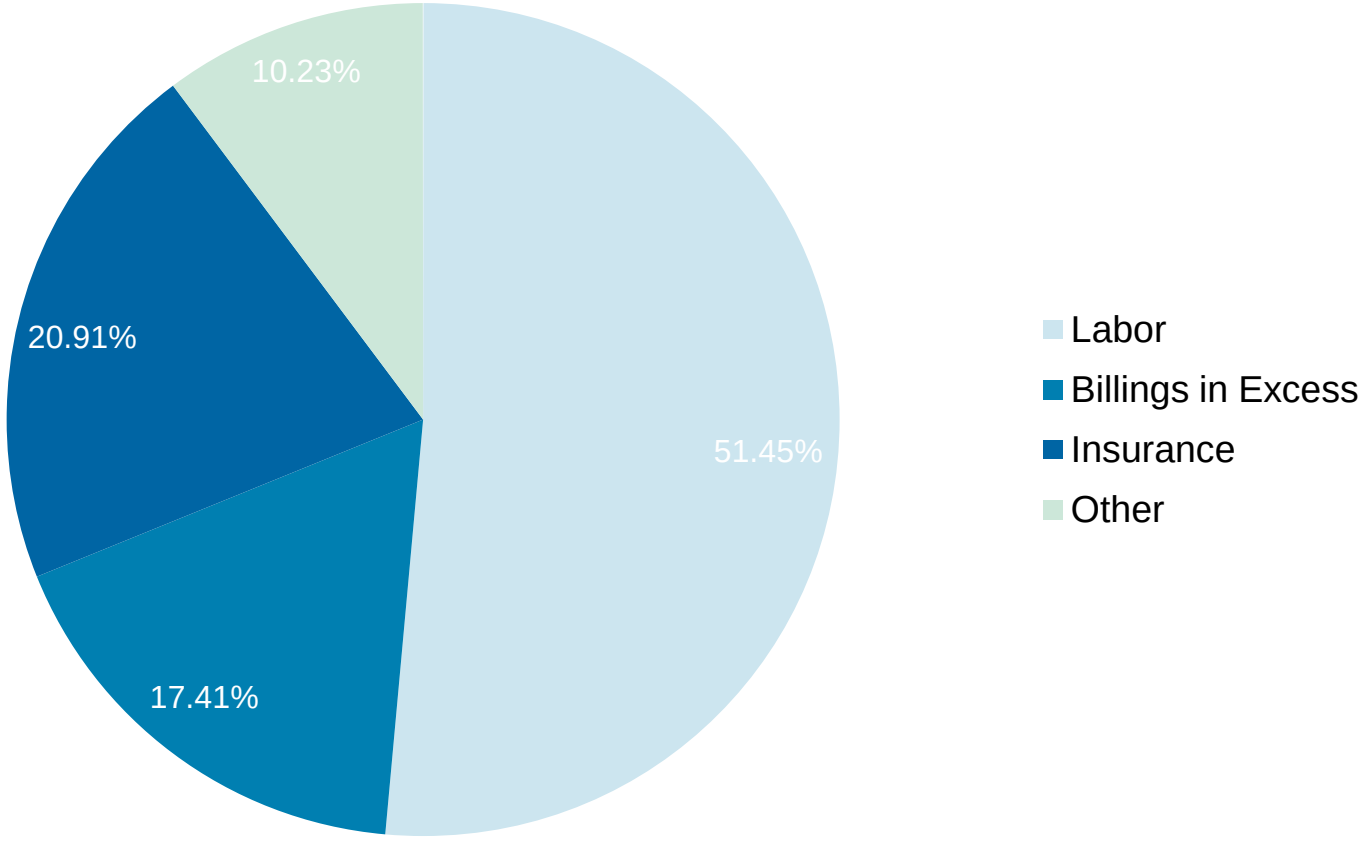

McGladrey

# Cost reimbursable – Current issues

- Labor
- Clean-up
- Negotiations
- Two trades
- Subcontractor
  - Self performed work – general conditions
- Insurance

McGladrey

# Over billings




McGladrey

# Thank you

**Patrick Hagan**
National State and Local Government Industry Leader
patrick.hagan@mcgladrey.com

**Jermaine Stanley**
Public Sector National Practice Manager
jermaine.stanley@mcgladrey.com

**Sharon Griffin**
Risk Advisory Services Director
sharon.griffin@mcgladrey.com

**John Croy**
National Leader Construction Risk Management
john.croy@mcgladrey.com

**Corbin DelCarlo**
Regional Leader Security and Privacy Services
corbin.delcarlo@mcgladrey.com

McGladrey

**McGladrey LLP**

800.274.3978
www.mcgladrey.com

McGladrey

Assurance ▪ Tax ▪ Consulting