AGC of Alaska NEWSLETTER

May 2020

AGC's Advocacy Efforts in Action

With the current health pandemic affecting day-to-day life and business, now more than ever, AGC is advocating on behalf of our members and working to provide them with the information and resources needed to continue building Alaska. Whether you are a general contractor, specialty contractor, or an associate member, your needs and interests come first at AGC of Alaska. Membership with AGC gives you the opportunity to engage with state legislators, government officials, and state and federal agencies that influence our industry. We actively promote our members' interests, protect their livelihoods, and represent them while keeping them abreast of the latest industry news, trends, business practices, and regulatory and legislative activities at both the state and national level.

On top of our typical advocacy efforts, some of AGC's direct COVID-response efforts have involved:

- Participation in a variety of working groups at the municipal/state levels to ensure the construction industry continues to remain classified as essential, and help shape mitigation and recovery efforts.
- Hosting a virtual agency day webinar for our members to engage in presentations from Alaska's Congressional Delegation, DOT and DOD (USACE) officials, MOA, and Fairbanks North Star Borough representatives, and more.
- Creation of AGC's COVID-19 Business Resource webpage for our members. Development of a COVID-19 Management Plan template for member businesses to use/reference to help mitigate the transmission of the coronavirus and provide safe and healthy working environments.

If you work with generals, subs or other supplier/service provider businesses that you feel could also benefit from AGC's aggressive advocacy work, please connect them with our membership director, Clare Kreilkamp to get them on board with all the benefits AGC has to offer.

Click on the link below to be taken to AGC's resource webpage for COVID-19 industry related updates:
https://www.agcak.org/COVID-19-RESOURCES.html.

Check out the AGC of America Podcast Series

ConstructorCast
The AGC of America Podcast

Inside this Issue

Special points of interest

- Click here to check out the AGC Online Calendar for updated information on Events & Training.
- If you have news or an event you'd like to share with other AGC members, email Kimberley@agcak.org.

FOR HEAVY FREIGHT SHIPMENTS
GO OFF-ROADING.

Seasonal highway weight restrictions can cause major problems when you need to move big volumes and heavy goods.
Keep your heavy freight off the road and on time with the Alaska Railroad.

Request a FREE quote: **800.321.6518** | AlaskaRailroad.com/freight

ALASKA
RAILROAD

AGC of America Multiemployer Pension Reform Update

AGC has been heavily engaged with the Administration and Congress as fiscal rescue packages are being developed. Thus far, those packages as you know have focused largely on addressing the health and economic fallout of COVID-19. That hasn't stopped AGC from advocating for issues directly impacting signatory contractors. AGC's advocacy includes addressing:

- Unique impact of the new federal paid leave mandates on signatory contractors;
- Affiliation rules and eligibility for PPP loans;
- Policies that will maintain the viability of multiemployer pension and health plans because of the negative impact of the market downturn and the compounded effect of diminishing hourly contributions.

The benefit fund concern is highlighted by a recent report from Milliman that states the multiemployer system's aggregate funding level is estimated to have dropped from 85% to 68% during the first 10 weeks of 2020 and another Milliman report earlier this week that focused on the impact of sustained contribution losses.

Specific to pensions AGC has been working with policymakers on pension relief that includes:
- funding to the PBGC for partition assistance for failing plans
- actuarial smoothing to protect the recent healthy plans hit by a drop in work hours
- authorization of Composite Plans

On the health and welfare side AGC has been calling for:
- COBRA premium assistance for workers who lost health coverage due to job loss or reduction in hours
- reinsurance for testing, treatment and prescription drugs from COVID-19

AGC, industry stakeholder groups, and the building trades continue to work together on many of these priorities. Unfortunately—despite what seems like endless spending by Congress—there does not appear to be bipartisan willingness to provide unlimited funding to the PBGC or make non-fiscal policy changes, like authorization of Composite Plans in the next round of COVID related legislation. Congressional leaders have pointed to the Phase III CARES package about direct funding for health care and stemming job losses. And Speaker Pelosi has dropped some of her insistence on pension relief in the next package which some have dubbed CARES 2.0 or Phase 3.5. On the positive side, there has been a growing acknowledgement of the growing multiemployer pension crisis and a commitment by the Trump administration and congressional leadership to address the issue, just no timeline yet. While it is possible legislation providing assistance to health and welfare plans could occur in the next round of legislation but that also remains very fluid we are targeting the next round of stimulus legislation to make a big pension push.

AGC Calls for Clarity of PPP Guidance

Set of AGC Webinars Scheduled on Topic

On April 29, AGC called on the Secretary of the Treasury (click here to view letter) to provide more clarity regarding its recent guidance warning firms of future audits and potential legal risks for companies that apply for loans. AGC is having discussions with key Administration officials on the impacts this guidance has had and ways it can be addressed. As this has created quite a bit of confusion, AGC sought to provide clarity to members through its ConstructorCast Coronavirus Special Report, which you can watch or listen to.

In addition, AGC is finalizing a pair of webinars on this and other questions regarding the Paycheck Protection Program:

May 6, 2:00 PM EDT: Paycheck Protection Program: Key Updates and Developments in the Ground Rules of the Program
May 7, 2:00 PM EDT: Paycheck Protection Program: Preparing Your Business Today for Audits, Oversight, and Agency Enforcement and Whistle Blower Actions Tomorrow

New Members

Generals

Alaska Commercial Contractors, Inc.
Doug Courtney, President
Jason Murdoch, Secretary/Treasurer
10221 Glacier Hwy.
Juneau, AK 99801
P| (907) 500-9993 ~ F| (907) 500-9994
doug@akcci.com ~ jason@akcci.com
www.akcci.com
Vertical commercial construction, renovation & new construction.

Genesis Construction LLC
Aaron Goodfellow, Owner
7634 E Sandstone Dr.
Wasilla, AK 99654
P| (907) 947-9191
agoodfellow@genesisak.com
www.genesisak.com
Light commercial build-out and tenant improvements. Anywhere from site excavation through framing and finish.

Specialty

Mountain Trucking, LLC
Julie Olson, Member
2149 Otter Dr.
North Pole, AK 99705
P| (907) 490-6550
mountaintrucking@gci.net
Aggregate hauling services, including sidedump, bellydump, and enddump, as well as equipment, freight, and hazmat statewide and Prudhoe Bay

SUMMIT Painting & Drywall, Inc.
Jeanine Graham, Vice President
Eric Graham, President
2557 Micah Rd.
North Pole, AK 99705
P| (907) 488-9489 ~ F| (907) 488-9484
summitpaintak@gmail.com
Painting & drywall applications

Associate

Linda Leary Consulting LLC
Linda Leary, Sole Proprietor
4011 Arctic Blvd., Unit C
Anchorage, AK 99503
P| (907) 306 3097
linda@llcak.com
www.llcak.com
Business Consulting

Associate - Continued

Northern Star Enterprises, Inc dba Superior Hardwoods
Justin Christian, Owner/Vice President
Nava Christian, Owner/President
600 Old Steese Hwy. N
Fairbanks, AK 99712
P| (907) 457-8351 ~ F| (907) 457-8352
info@shwalaska.com
https://shwalaska.com
Retail hardwood lumber and custom millwork

US DOL Adds to Emergency Paid Leave Q&A's and Begins Enforcement

Temporary Non-Enforcement Period Ended April 17

The U.S. Department of Labor's Wage and Hour Division (WHD) recently added a number of new "Questions and Answers" to provide information to employers about meeting their requirements to offer emergency paid sick leave and paid family medical leave offered by the Families First Coronavirus Response Act (FFCRA). The new Q&A's further address critical questions, such as how to count hours for employees with irregular hours; how to compute average regular rate; how employers can require usage of existing leave; implications of stay-at-home and shelter-in-place orders; and future enforcement implications. Click here to learn more.

US DOL Publishes Emergency Paid Leave Regulations

Treasury Issues Tax Credit FAQs

The U.S. Department of Labor today announced new action regarding how American workers and employers will benefit from the protections and relief offered by the Emergency Paid Sick Leave Act and Emergency Family and Medical Leave Expansion Act, both part of the Families First Coronavirus Response Act (FFCRA). The department's Wage and Hour Division (WHD) posted a temporary rule issuing regulations pursuant to this new law, effective today, April 1, 2020. Click here to learn more.

ANNIVERSARIES

GENERAL

GREAT NORTHWEST, INC. - 36
PRUHS CORPORATION - 24
ROGER HICKEL CONTRACTING, INC. - 20
NANUQ, INC. - 14
ALBORN CONSTRUCTION, INC. - 12
DRENNON CONSTRUCTION & CONSULTING, INC. - 12
RESTORATION SCIENCE & ENGINEERING - 10
KUCHAR CONSTRUCTION, LLC - 8
TURNAGAIN MARINE CONSTRUCTION - 6

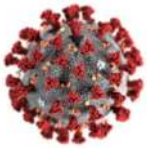
SPECIALTY

NORCOAST MECHANICAL, INC. - 32
FULLFORD ELECTRIC, INC. - 18
COLDFOOT ENVIRONMENTAL SERVICES, INC - 15
EP ROOFING, INC. - 13
MCKENNA BROTHERS PAVING, INC- 12
KLEBS MECHANICAL, INC. - 10
GMW FIRE PROTECTION, INC. - 7
5150 GLOBAL SOLUTIONS, LLC - 4
BOARD OF TRADE, INC. - 3
G&S MANAGEMENT SERVICES, LLC - 1
KAE, INC. - 1

ASSOCIATE

N C MACHINERY CO. - 71
MARSH & MCLENNAN AGENCY - 60
SENCO ALASKA, INC. - 45
ALASKA RUBBER GROUP - 32
OLES MORRISON RINKER & BAKER, LLP - 29
RICHARDS PIPE & STEEL, INC. - 26
ALLIED STEEL CONSTRUCTION, INC. - 23
ALASKA PURE WATER PRODUCTS - 20
ROTATING SERVICES, LLC - 16
CHEVROLET OF SOUTH ANCHORAGE - 13
LIFEWATER ENGINEERING COMPANY - 12
ALASKA STATE CHAMBER OF COMMERCE - 11
ALASKA NATIVE TRIBAL HEALTH CONSORTIUM—ANTHC - 10
ARC PACIFIC NORTHWEST - 10
ATCO STRUCTURES & LOGISTICS - 9
CORE & MAIN - 8
THE LAKEFRONT ANCHORAGE HOTEL - 7
HILCORP ALASKA, LLC - 6
UAF CTC CONSTRUCTION MANAGEMENT PROGRAM - 6
VICTAULIC COMPANY - 5
BRADISON MANAGEMENT GROUP - 4
ALASKA PRINTING, INC. - 3
ALASKA PIPE SPECIALISTS - 1
BEADEDSTREAM, LLC - 1

LINKS of Interest



COVID-19 Resources

AGC of Alaska COVID-19

Reopen Alaska Responsibly Plan

Municipality of Anchorage COVID-19 Business Dashboard

COVID-19: Anchorage Economic Recovery and Resiliency
Resources and information from Mayor Berkowitz's Economic Resiliency Task Force

Links to Resources for Business Owners, Employees, Non-Profits, & Residents Looking for Help

Critical Infrastructure Template COVID-19 Management Plan

THANK YOU!

Virtual Agency Day Webinar

We would like to thank all the panelists and attendees who joined us for our first ever Virtual Agency Day Webinar on April 16th via Zoom. It was great to hear from Congressman Don Young, Senator Dan Sullivan and Senator Lisa Murkowski, as well as representatives from the Department of Transportation, the US Army Corps of Engineers, Fairbanks North Star Borough & the Municipality of Anchorage.

Click here to view the available handouts and Zoom recordings.

New Labor Agreements!

AGC mediates labor agreement negotiations between industry representatives and union representatives, and members benefit greatly from the 'strength-in-members' negotiating position provided by the association. These negotiated agreements are utilized by the State of Alaska to determine prevailing wage requirements for public projects. AGC posted the new Collective Bargaining Agreement for the Teamsters and Technical Engineers Local 959, International Union of Operating Engineers Operative Plasterers Local 302 and Cement Masons MOU. Keep an eye on AGC's on AGC's Labor Agreements webpage page as we expect to post the new Council of Laborers agreement in the near future.

4 Ways Contractors Can Get Federal Relief During COVID-19

By Daniel Wilson

Law360 (April 24, 2020, 9:26 PM EDT) -- Policies allowing federal contractors to claim costs for employees unable to work, accelerating payments for work in progress, and providing billions of dollars in loans for small business are among the most influential federal contracting changes stemming from the COVID-19 crisis.

Alongside an unprecedented coronavirus rescue package, federal agencies have also introduced a slew of new contracting regulations, guidance, class deviations and other changes intended to help ensure essential items and services are quickly produced and get where they need to be — and to help ensure that important parts of the federal supply chain don't go out of business.
At the same time, certain existing contracting laws and regulations such as contract change clauses in the Federal Acquisition Regulation, or FAR, are also becoming more prevalent.
Here, Law360 examines four coronavirus-related contracting policies that federal contractors need to be aware of. Click here to read on!

Certified Tower Climbing and Rescue Occupational Certification Program

Upcoming Training Dates: May 7-8, May 21-22, and June 16-17

The Tower Climbing and Rescue curriculum was developed specifically for Alaskan climbing conditions. This course meets ANSI/ASSE and OSHA Criteria for Accepted Practices in Health, Safety, and Environmental training and authorizes the worker as a climber and assisted rescuer for tower climbing. Click here for more information!

AGC Alaska's Interview with Deep Forest Security Consulting—Answering our Cyber Security Questions on Protecting your Data!

Q: What are some of the most common mistakes that companies make that increases their risk of becoming a victim of cybercrime?

A: Most companies are focused on providing goods and services to their clients, and earning revenue … and rightly so, because this is how we keep the doors open! But quite often, leaders don't pay the same amount of attention to the welfare of their computer systems, which have become critical to ensuring business operations. This lack of awareness can also drive the false conclusion that "it won't happen to me because I'm so small or different." The truth is, a security weakness in a military system looks identical to one in a public library, and most often both are attacked equally. If your company is connected to the Internet, you're absolutely a target. Aside from this, here are the top mistakes we see companies making:

1. *Unintentional delegation of cybersecurity to IT.* When asked about cybersecurity, many business owners respond, "Our IT department takes care of it." I say "unintentional delegation" because in many cases, especially when IT is outsourced, we find that there are no metrics for cybersecurity in job requirements or contracts. Many CEO/CIO's are concerned about security, but haven't discussed with IT exactly how it's being accomplished.
2. *Operational Focus of IT.* IT admins, almost without exception, are resource constrained and barely able to keep up with the operational needs of the business. Thus, when faced with a choice of "Do I fix the bookkeeper's broken PC, or do I review security logs?" any wise sysadmin is going to fix the broken PC, because the business must continue to function. Ultimately, security takes a back-seat because it's not been made a priority.
3. *Lack of Expertise.* Even in the rare cases where IT has enough resources to perform security related functions, most IT administrators don't have the training and experience needed to truly assess risk and develop cost-effective, efficient, mitigating solutions. At best, the company ends up with ad-hoc solutions for specific issues, not the overall security management plan that's needed.
4. *Lack of a Security Management Program*. Many businesses have programs to ensure employee safety that include components like training, testing, and risk assessment and mitigation efforts. Yet, most companies don't have a similar program for cybersecurity that evaluates the importance of information, assesses threats, likelihoods, and impacts to the business if that information is compromised or destroyed, and prescribes controls to reduce those risks. Just like you wouldn't train someone on how to climb a ladder safely but not how to tie off when on a roof, an incoherent or incomplete cybersecurity program can be just as disastrous because of the false sense of security.
5. *No Cyber Insurance Policy.* Many companies still don't have a data-breach/cyber-incident insurance policy. When something bad happens, a policy that covers incident response costs will dramatically reduce your stress and improve your business' chance of successful recovery.

Q: What are the top 6 things I should be doing to protect my data?

A: Every cybersecurity expert will start off by saying "have good backups," and they're not wrong. But reality is more complicated than this. We've responded to several incidents (i.e. We're called in to clean up the mess once the barn has burned down) where the client "had good backups." But, the badguys found those backups and destroyed them before encrypting everything and demanding a ransom. The most effective way to mitigate risk for every environment is to develop and implement a security management program. This sounds vague, expensive and hard to do, but it doesn't have to be. It does, however, require training and experience to do right. Here are some of the main components of an effective security management program:

1. *Obtain Executive Support.* Effective cybersecurity must be based upon risk and if done right, costs will be commensurate with the risk. You don't want to spend $100 to protect information worth $10. Conversely, spending $1 to protect $100,000 is not realistic either. Still, business leadership must be supportive of any security effort for it to be successful as a loss-prevention and business enablement program instead of failing as a cost center.
2. *Perform a Risk Analysis.* Inventory the different types of information in your environment. For example, contracts and bids, employee/HR, proprietary designs and processes, accounting, etc. For each type of information, determine what the impact to your business would be if it were compromised, altered, or destroyed. Finally, based upon an analysis of possible threats to your information, determine overall risk. While I've oversimplified things for brevity, there are several methods for doing this, with some easier than others. Deep Forest Security uses a hybrid method we've developed over many years that's based upon methodologies from the National Institute of Standards and Technology

(NIST), and the National Security Agency's Infosec Assessment Methodology (NSA IAM). These are great resources for security nerds; they also cure insomnia in everyone else.

3. *Assess Vulnerabilities.* It's hard to know everywhere to look for vulnerabilities that could impact your information; the risk analysis effort will help with this. At a minimum, you'll need to examine your network, both internally and externally, for technical vulnerabilities as well as look at policies and procedures for nontechnical issues. Technical vulnerabilities must be reassessed no less than every 3 months (at DFS we do this weekly), and policies and procedures reviewed no less than annually to start with.
4. *Implement Security Controls.* Identify exposures that existing security controls don't cover, and install new solutions to mitigate the remaining risks. In some cases, mitigating a risk won't be reasonable or appropriate, and should be accepted in writing by executive leadership. Accepting risk is a tricky thing, and guidance from persons experienced in cybersecurity risk management is critical.
5. *Rinse, Repeat.* Steps 1 – 4 must be repeated periodically to ensure the security management program remains effective and efficient. Executives must be periodically updated on current and evolving risks and vulnerabilities. Networks and computers must be checked often for new vulnerabilities. Policies and procedures must be reviewed to ensure they still meet business needs and address nontechnical risks.
6. Steps 1 -5 really lay out the components of an effective security management at a high level: Get leadership on board, figure out where you are, fix things, and re-assess. Every aspect of information security can be mapped to one of these steps. Many of the required steps are difficult to execute without training and experience, and some absolutely require it. Call or email us if you need help, or if you just want a second opinion on your current security protections.

In every talk and article, I like to leave readers and audiences with some hard, actionable steps to take. So, above all else, I would tell businesses to *have good backups!*

Q: What can we do to detect hackers trying to break in?

A: One of the most effective, and crucial, components of a security program is log monitoring. By configuring your servers, desktops, firewalls, and other equipment to send security logs to a single location, you can monitor those logs for events that can provide clues that an attack is imminent or underway. For example, if you detect numerous login failures on your website employee portal, you can block the attacker at the firewall, or require everyone to change their passwords as a safety measure. But, if you're not looking at logs, there's no way to know this is happening; I can guarantee it's happening. All day, every day, to everyone.

The challenge is that machines generate enormous amounts of log records, making it impossible for any human to review them, and even if they could, reviewing logs once a week is not sufficient to respond to an attack – the badguys will have already gained access. Furthermore, automated solutions are expensive and hard to install without training and experience.

Log monitoring and alerting is something we've seen as a challenge for almost all of our clients for the past 15 years. So much so, that in 2018 we started providing this capability as a managed service, at about ½ the cost of what a single security administrator would cost, and a fraction of what purchasing an in-house solution can cost. Furthermore, logs are reviewed by analysts that have actual incident response training and experience, which dramatically increases the changes of detecting badguys before they can do damage.

Q: What is the first thing I should do if I believe my server or system has been compromised?

A: Any company who has had their network compromised by bad people, will tell you that it was one of the worst experiences of their lives. The sudden plunge into chaos, the stress of worrying if the compromise will close the business; the stress of dealing with law enforcement, the concerns over what data was compromised and what the consequences will be, all add up to a very, very bad day.

Cyber intrusions happen frequently. They happen to businesses of all sizes and industries. Sadly, we meet many good people in the midst of watching their professional word burn down around them. The reality is that if you did not have appropriate cyber security measures in place, the results may be worse than need be, and it will absolutely cost more money than necessary.

Having the right people on your response team can make a difference. Call a qualified Cyber Security Specialist

immediately. If they are local, they can respond quickly and can provide incident command leadership to deal with the crisis and produce the best outcome possible. If law enforcement is involved, they will also have the experience to work with both federal and local law enforcement, and ensure your best interest is served. They can also assist with the cyber forensics efforts in discovering where the compromise originated and how it breached your system.

Q: Is it true that cyber-attacks have increased with the COVID-19 coronavirus pandemic?

A: Yes. The COVID-19 "shut down" created a unique business environment, in which businesses that could, scrambled to put tools in place for employees to work from home. In response, the badguys ramped up their efforts to take advantage of vulnerabilities this new paradigm created from hastily assembled remote access solutions. According to the Department of Homeland Security, the badguys increased their targeting of at-home computers and remote access by over 600%!

The problem arises from a false sense of security companies get when utilizing remote access. While the corporate network has firewalls, VPNs, antivirus software, and zealous IT admins, protections around at-home computers are almost always far less substantial. This makes them perfect targets for hackers. Once the at-home computer is compromised, badguys steal passwords and infiltrate the corporate network. Unfortunately, we've already seen this happen to companies here in Alaska and the Pacific Northwest.

Q: We often hear what we should or shouldn't do at work with our security, but is there anything we should be doing at home as well?

A: Aside from the usual "be sure your antivirus software is up to date and have a firewall," we are strongly encouraging everyone to be exceptionally sensitive to the emails they receive, as email-based attacks are the single most effective method an attacker has for compromising a machine. DFS gives a really fun talk on the mechanics of phishing and the specific tactics used by badguys to get readers to click the link or open the attachment. Some tips included in our talk:

1. Pay attention to From: email addresses. If you get an email alert from Bank of America, but the From: address is bankofamerica-alerts@gmail.com, this is a clue that the email is fake.
2. Never, ever, click on links provided in email alerts. If PayPal sends you an alert that your account has been locked, open a browser and type in 'www.paypal.com'. The email may be legitimate, but don't risk it by clicking on the embedded link, because if you're wrong, your computer will likely be compromised and/or encrypted for ransom.
3. Pay attention to the writing style of the message. Did you receive an email from your boss telling you to wire money to a new vendor, but is written differently than he typically does? For example, if Mr. Boss always signs his email with "Regards, Bob" and the email says, "Blesings be Upon You," that's a clue. Give Mr. Boss a quick call or text to verify.
4. Avoid opening attachments, especially if #1-3 above may apply. You can usually verify if an email is legitimate by sending a quick text to the purported sender.
5. If an email contains an "emergency," read it carefully. If you must reply immediately to avoid your account being locked, it's almost certainly a phishing attack. Follow #2 above.
6. Don't click on pictures of Russian women looking for friendship, don't reply to Nigerian widows needing to exfiltrate money, and ignore emails from the IRS, Social Security Administration, the FBI, and any other government agency. If it's really legitimate, they'll call you or visit you in person.

In addition to this, try to limit general non-business Internet usage of your at-home computer while working remotely to limit the chances of it being compromised from a poisoned website.

Q: Any closing thoughts?

A: There are so many facets to information security that it can feel like drinking from a firehose. Don't be discouraged or dissuaded from tackling the beast though. You eat an elephant one bite at a time. If you need help with anything cyber-security related, or just want an opinion or guidance, please call or email us. Deep Forest Security is dedicated to protecting our fellow Alaskan businesses, and we relish every battle won against the badguys.

Mike Messick is the owner of Deep Forest Security Consulting, located in Anchorage, Alaska. Mike has 30 years of information security consulting experience in Fortune 5 enterprises, Internet Service Providers (ISPs), and independent consulting. Founded in 2005 originally as Digital Securus, Deep Forest Security provides risk-based information security consulting and managed services to clients within Healthcare, Government, Financial, Oil & Gas, Energy, Construction, Transportation, and other industry sectors. CMMC cyber security paradigm. Deep Forest Security can be reached at info@deepforestsecurity.com, or (907) 334-9090 ext. 101.