Cybersecurity Forum 2020

The Threats to You, Your Company and the Economy & Complying with the Cybersecurity Maturity Model Certification (CMMC) Standards

Presented In Partnership Between

WCI Workers' Compensation Institute

AIF Foundation

DEO Florida Department of Economic Opportunity

U.S. Department of Defense Office of Economic Adjustment

FloridaMakes

September 16 & 17, 2020

Presented virtually.

Keynote Speaker
U.S. Senator Marco Rubio

Senator Rubio will present a compelling overview of the national risks associated with cyber breaches from other nation states. As Chair of the U.S. Senate Committee on Small Business and Entrepreneurship, Acting Chair of the U.S. Senate Intelligence Committee, and Committee member of the Foreign Relations and the Commerce Science and Transportation Committees, he is in a unique position to understand and explain security risks that need to be closely overseen.

Featuring
Katherine "Katie" Arrington

As the Chief Information Security Officer (CISO) to the Assistant Secretary of Defense for Acquisition, Ms. Arrington is leading efforts that will help to ensure a robust Supply Chain Risk Management (SCRM), establish defense industrial base security and resilience, and create a common basis for cybersecurity standards. The Department of Defense is in the process of implementing the new Cybersecurity Maturity Model Certification (CMMC) standards and Ms. Arrington will give attendees an update on the timelines, the certification process, and the impact to industry.

The Cybersecurity Forum 2020, originally scheduled as "in-person" breakout sessions at the Annual Workers' Compensation Educational Conference sponsored by the Workers' Compensation Institute (WCI) has been *rescheduled for September 16–17, 2020.* As a result of the COVID-19 pandemic, the annual WC Conference was postponed until 2021. However, because of the importance and urgency of the Cybersecurity sessions, WCI has elected to present them virtually this year. A follow up to these initial sessions will be held at the 2021 Educational Conference.

Why Attend?

Cyber attacks and data breaches are on the rise. This affects us as individuals, our companies, and is a serious national security threat to our country. Whether you are seeking a "best practices" approach to providing cybersecurity or will be required to meet the new federally mandated standards that for some become effective in 2020, this series of educational offerings provides a current model for responding to real cybersecurity risks that involve all aspects of our society.

What You Will Learn:

Day One

- How to protect your data – Individuals and Companies
- Who are the "bad guys"?
- How to recognize and respond to a cyber breach
- Witness a Simulated Cyber Breach
- Preventative action steps for protection
- Senator Marco Rubio's keynote address about the importance of cybersecurity nationally and internationally
- Are we prepared for a cyber attack on our critical infrastructures (energy, transportation, port access, communications, health services, utilities, information technology, and defense systems) and what will Florida look like if there is a breach resulting in a shutdown in whole or in part?

Day Two

- These sessions will inform all companies in the defense supply chain of the U.S. Department of Defense's Cybersecurity Maturity Model Certification Program (CMMC) that is expected to be in effect for some in 2020.
- Educational sessions will be presented on compliance with CMMC standards by Board Members and DoD staff who actually authored these new standards.
- The Keynote Address for this day's sessions will be made by Katherine "Katie" Arrington, the Chief Information Officer (CISO) to the Assistant Secretary of Defense for Acquisition, in regards to the DoD's expectations for CMMC.

Who Should Attend?

Some estimate that in excess of 300,000 companies/individuals will qualify as being subject to the mandatory CMMC Standards required by the Department of Defense. Understanding your possible newly defined obligations is essential for good business planning and will be important for future planning as these new standards are expanded to other Federal agency requirements. Those that should attend include:

- Small and mid-sized Florida Defense Contractors as defined by CMMC
- Companies in the Defense Industrial Base as defined by CMMC
- IT Professionals and Risk Managers responsible for the development of company processes in compliance with CMMC or best practices
- Safety Professionals in regards to ensuring total company compliance related to cybersecurity
- PEOs and Temporary Staffing Companies providing services to companies in the DoD supply chain
- Any Individual or Company providing services or products to companies within the defense supply chain
- Prime Contractors seeking resiliency through ensuring that supply chain providers of services/products have the appropriate cybersecurity certifications
- Attorneys including Company Staff Attorneys providing advice on cybersecurity standards and potential liability for first and third party liabilities
- HR Professionals dealing with confidential or protected data
- Claims Adjusters receiving certain types of confidential or unclassified protected data as a part of their job functions
- Insurance Carriers/Self-Insureds/Third Party Administrators (Liability coverages for risks related to cyber breaches) and the need for data protection including information received in underwriting activities
- Companies and Individuals seeking information on "best practices" for cybersecurity
- Company Managers overseeing the conduct of employees for the purpose of protecting data (cybersecurity risks are the concerns of the entire company not just a few)
- Companies desiring to do business planning for Florida operations and the overall risks of a cyber breach (or for that matter any catastrophic event) on the state's critical infrastructures

Program Agenda

These series of sessions provide industry with updated cybersecurity information as related to the causes of cyber breaches, the liabilities that a cyber breach can cause, industry's appropriate responses to a breach or suspected breach, the efforts made by third parties to obtain data maintained in a cyber platform and the predictability of a cyber breach's effect on the national economy should there be a significant breach of the nation's critical infrastructure. Of perhaps more significance is the understanding of efforts made by other nations to obtain our military and other protected data. U.S. Senator Marco Rubio (Florida) will provide an updated report on national cyber breaches attempting to obtain protected data of national concern.

Wednesday, September 16, 2020

Recognizing and Dealing with Cyber Breaches

8:45 – 9:00 am **Opening Remarks/Welcome**

James N. McConnaughhay
McConnaughhay, Coonrod, Pope, Weaver & Stern, P.A.
Chair, Workers' Compensation Institute
Tallahassee, FL

Welcome/Introduction of Speakers

Tom Feeney
CEO
Associated Industries of Florida
Tallahassee, FL

9:00 – 10:00 am **The Long View on Cybersecurity**

Moderator:
Travis Rosiek
Chief Technology and Strategy Officer
BluVector
Arlington, VA

Speakers:
Bob Lentz
President, Cybersecurity Strategies;
Former Deputy Assistant Secretary of Defense, Cyber Identity and Information Assurance (CIIA)
Tampa, FL

Jan Tighe
Vice Admiral (Retired); Former Commander of Tenth Fleet/US Fleet Cyber Command;
Former Deputy Chief of Naval Operations, Information Warfare
Fort Lauderdale, FL

Major General (Retired) Joseph Brendler
Former Chief of Staff
US Cyber Command
Fairfax County, VA

Bill Sweeney
Distinguished Engineer
Comcast
Philadelphia, PA

Cyber attacks are becoming more frequent and getting more costly, complex and dangerous. New cybersecurity programs (like CMMC) are designed for protecting the industrial base today and in the future. In this resource-constrained environment (like IT budgets; a shortage of IT talent) how can companies prepare to meet these requirements? This session will include leaders who have long served in the cybersecurity arenas from technologists and R and D specialists to policymakers. They will provide perspectives of how we got here, what known and unknown threats (and opportunities) are on the horizon and how companies can best leverage solutions like artificial intelligence and machine learning to protect their companies.

10:00 – 10:15 am **Networking Break**

10:15 – 11:15 am **The Legal and Personal Financial Risks of Cyber Breaches**

Introductions/Moderator:
Julie Fetherman
Associate Executive Director
Workers' Compensation Institute
Tallahassee, FL

Presenters:
David Altmaier
Florida Insurance Commissioner
Tallahassee, FL

Robert A. Stines, *Attorney*
Freeborn & Peters, LLP
Tampa, FL

Michelle Chia
Head of Professional Liability and Cyber
Zurich North America
New York, NY

This session will include a case law update on legal liabilities assumed when a security breach occurs as a result of your employees or employees of a subcontractor being the cause of such. There is no question that the company causing a breach can certainly suffer damages from an individual standpoint. But what about liabilities to third parties based upon tort or contractual obligations? Following this presentation, the question arises as to whether insurance coverage can be purchased to protect an organization's financial exposure resulting from such a cyber breach. No other industry is affected by cybersecurity issues more than insurance. If a cyber breach occurs and results in damages to a company defined as an "insured" under a policy of insurance, does the policy of insurance pay for these damages? If as a result of a breach, damages result to third parties, are such liabilities covered? The Florida Insurance Commissioner will comment on various issues as related to insurance coverages applicable to Cyber breaches.

11:15 – 11:30 am **Networking Break**

11:30 – 12:30 pm Cyber Breach: The Real Thing and its Expected Impact

Moderator:
Tom Feeney
CEO
Associated Industries of Florida
Tallahassee, FL

Speakers:
Sergio Heker
Chief Executive Officer
GLESEC
Altamonte Springs, FL

Ami Braun
Vice President for Business Development
GLESEC
Altamonte Springs, FL

Christopher P. Cleary
Department of the Navy
Chief Information Security Officer (CISO)
Director of the Cybersecurity Directorate
Washington, DC

No cyber breach can be appreciated and completely understood without actually seeing an example of a breach. This demonstration will provide attendees with a look at a "breach" which will include a narration of what is taking place and the possible responses. This session provides a unique experience if you have never been involved with the details and possible consequences of a systemic cyber breach. Predicting the consequences of a cyber breach is not an "exact science" but it is important for business planning to appreciate its potential effects. Just like advanced planning for any natural disaster (such as a hurricane, pandemic, tornado, etc.), this session includes a presentation on the U.S. Navy's prediction of the consequences of a cyber attack on Florida's critical infrastructure. Any business sustainability plan should include planning for such an event.

12:30 – 1:00 pm Networking Break

1:00 – 2:00 pm Introduction of Supporting Attendees and Speaker

Tom Feeney
CEO
Associated Industries of Florida
Tallahassee, FL

Beverly Seay
Chair
Board of Trustees,
University of Central Florida
Orlando, FL

Jimmy Patronis
Chief Financial Officer
State of Florida
Tallahassee, FL

Speaker:
Senator Marco Rubio
U.S. Senator (Florida)
Miami, FL

Tom Feeney, CEO of Associated Industries, recognizes two of our supporting attendees without whose encouragement this Cybersecurity Forum would have been difficult to present. Senator Rubio will present a compelling overview of the national risks associated with cyber breaches by other nation states. As Chairman of the U.S. Senate Committee on Small Business and Entrepreneurship, Acting Chairman of the Select Committee on Intelligence, and Committee member of the Foreign Relations Committee and the Committee on Commerce Science and Transportation, he is in a unique position to understand and explain security risks that need to be closely overseen when dealing with other countries.

2:00 – 2:15 pm Networking break

2:15 – 3:15 pm Are We Prepared for a National Crippling Cyberattack? Lessons learned from the Pandemic Crisis

Introductions:
Tom Feeney
CEO
Associated Industries of Florida
Tallahassee, FL

Speakers:
Eric Noonan
CyberSheath Services International, LLC
Reston, VA

Paul Anderson
President and Chief Executive Officer
Port Tampa Bay
Tampa, FL

Michael Wee
Cyber Systems Engineer
Northrop Grumman
Falls Church, VA

Are the national reactions to the Coronavirus indicative of what will happen if there is a closure of critical infrastructures caused by a cyber attack? Even though the U.S. is the most technologically advanced country in the world, or we are the strongest and wealthiest nation still is in need of better "state of the art" cybersecurity planning and organization. A recently appointed congressional commission, in recognizing the potentially devastating effects of the national structure as a result of security breaches concluded, in summary, that better planning and preparation for foreseeable threats and disasters are needed. This panel will discuss issues as related to these concerns and the importance of planning for their industries.

3:15 – 3:30 pm Networking Break

3:30 – 4:30 pm Cybersecurity and the Space Industry: Introduction to CMMC, the New Cybersecurity Standards

Moderator/Speaker:
Ryan Bonner
Michigan Manufacturing Technology Center
Ann Arbor, MI

Speakers:
Frank DiBello
President and CEO
Space Florida
Cape Canaveral, FL

Vice Admiral John McConnell (U.S. Navy Retired)
Former Director of National Security Agency
Executive Director of Cyber Florida at USF
Tampa, FL

Huge opportunities including job creations are available for the advancement of the space industry. With these new opportunities comes the added significance for providing increased cybersecurity. Frank DiBello, as President and CEO of Space Florida, the aerospace economic agency of the State of Florida, is in a unique position to provide valuable information on the importance of these new developments with specific reference to cybersecurity. This presentation also serves as an introduction to the second day sessions that provide details for compliance with the new standards that will become effective in 2020 for companies within the "Defense Supply Chain."

4:30 – 5:00 pm Closing "reception" (virtual networking)

Thursday, September 17, 2020

Establishing a Certified Cybersecurity Program

Due to the continued threat of security breaches, the U.S. Department of Defense (DoD) is developing a new standard for cybersecurity for all organizations in the defense supply chain known as the Cybersecurity Maturity Model Certification (CMMC). Implementation is set to begin in 2020. Organizations in the DoD's supply chain will now have to achieve an appropriate CMMC certification level through assessment/audit by a neutral, properly accredited, third party entity. Currently, DoD contractors self-certify compliance with these amended cybersecurity standards. The mandatory compliance with CMMC affects not only the prime DoD contractors but also subcontractors, vendors, service providers and suppliers to companies within the supply chain. Of particular concern is the cost of the preparation, audit, and certification for small and medium sized businesses.

Facilitator:
Ryan Bonner
Michigan Manufacturing Technology Center
Ann Arbor, MI

7:30 – 8:00 am **Registration/Networking**

8:00 – 8:10 am **Welcome and Introduction of Speaker**

Kevin Carr
Chief Executive Officer
FloridaMakes
Orlando, FL

8:10 – 9:10 am **Keynote Speaker - Perspectives from the Department of Defense on the new CMMC Standards**

Katherine "Katie" Arrington
Chief Information Security Officer within the Office of the Secretary of Defense For Acquisition and Sustainment
Washington, DC

How the Department of Defense views the new CMMC Standards is paramount in determining what will be needed for compliance. What information is being protected and fits within the definition of "controlled unclassified information" (CUI)? What companies will be considered within the "defense supply chain" for mandatory compliance? What role must a prime defense contractor play in ensuring that its subcontractors, service and product providers and other related companies be compliant and what is the effect of non-compliance on an award of contracts in the first instance and the continued ability to do business with the Department of Defense thereafter? These questions and many more will be best answered by Ms. Katherine "Katie" Arrington, Chief Information Security Officer within the Office of the Secretary of Defense for Acquisition and Sustainment. Ms. Arrington provides a unique experience for attendees by explaining in detail exactly what the Department of Defense's expectations are and the processes that will be followed in the oversight of compliance.

9:10 – 9:30 am **Networking Break**

9:30 – 11:00 am **Perspectives from the CMMC Accreditation Body (Panel)**

Moderator:
Ryan Bonner
Michigan Manufacturing Technology Center
Ann Arbor, MI

Panelists:
Karlton D. Johnson
CMMC-AB Board of Directors,Vice- Chair
Delaine Strategy Group, LLC
Purcellville, VA

Jeff Dalton
CMMC-AB Board of Directors,
Accreditation and Credentialing Committee Chair
President and CISO
Broadsword Solutions
Marathon, FL

Tim Rudolf
CMMC-AB Board of Directors,
Nominations and Governance Committee Chair
Alexandria, VA

Chris Golden
CMMC-AB Board of Directors
Infrastructure Committee, Co-Chair
Finance Committee, Co-Chair
Washington, DC

The Accreditation Body of CMMC (CMMC-AB) is a non-profit independent institution created to manage, control and administer the CMMC certification process within the Defense Industrial Base. This panel of CMMC-AB Board Members will discuss the overall journey from idea to operation in the development of the CMMC Accreditation Body and the relevant technical specifications. They will address the processes for CMMC certification, licensing of assessors to perform CMMC Assessments or how to become a Certified Third-Party Assessor Organization (C3PAO),conduct training, and operate the CMMC Ecosystem. It is essential for those required to certify with the CMMC standard to be fully apprised of these new processes and the role of the CMMC-AB. Additionally the panel will explain the process through which partnership arrangements are developed and some opportunities that exist for partners within the CMMC Ecosystem.

11:00 – 11:10 am **Break**

11:10 – 11:30 am **Cybersecurity Impacts to Florida**

Congressman Michael Waltz
(Florida District 6)
Palm Coast/ Deland/ Port Orange, FL

As a current member of the Committee on Science, Space and Technology and the Intelligence, Emerging Threats and Capabilities Subcommittee, Congressman Waltz will update our Forum participants with some important insight on the steps that Congress is taking to protect the country from both national and international cyber threats and what we can do to minimize our vulnerability to those risks.

11:30 – 12:30 pm **CMMC Challenges and Opportunities-How will CMMC Affect the Florida Economy?**

Moderator and Introduction of Panelists:
Ryan Fierst
Senior Management Analyst
Division of Strategic Business Development
Florida Department of Economic Development
Tallahassee, FL

Panelists:
Dale Ketcham
VP Government & External Relations
Space Florida
Exploration Park, FL

Sid Kaul
CIO
All Points Logistics
Houston, TX

Robert Abascal
President
AVT Simulation
Orlando, FL

Paul Sohl
Rear Adm. U.S. Navy (retired)
CEO
Florida High Tech Corridor Council
Heathrow, FL

This session will be the kick-off of DEO's Cyber Training grants program which will cover such questions as: How does my business get started with CMMC implementation? What should we focus on first? How do we achieve the greatest impact at the least amount of costs? Who is impacted by CMMC? What information is considered protected by CMMC? This panel reflects Florida profiles from both the Florida government and defense sectors, Florida small/mid-size business owners, and the military.

12:30 – 1:00 pm **Break**

1:00 – 2:30 pm **Mapping the CMMC Journey – from Concept to Certification**

Speaker:
Ryan Bonner
Michigan Manufacturing Technology Center
Ann Arbor, MI

This interactive "workshop session" will include an overview of the major phases all organizations go through as they pursue implementation of the CMMC model. Topics will include:

- Inventory and scoping of controlled unclassified information/federal contract information
- Readiness assessments of CMMC domain capabilities
- Identifying and remediating gaps in cybersecurity practices
- Preparing for and supporting the assessment process

2:30 – 3:00 pm **Closing "Networking" Reception**

Direct inquiries regarding continuing education to WCI – (850) 425-8156.

Current Sponsors

CYBERSHEATH SERVICES INTERNATIONAL
ENSCO 50 Years of Ideas to Reality
DUKE ENERGY
All Points
BLUVECTOR A COMCAST COMPANY
WCI Workers' Compensation Institute
FLORIDA DEFENSE ALLIANCE
READY CERT
FIC FLORIDA INSURANCE COUNCIL Covering Florida Since 1962
AIF IT ASSOCIATED INDUSTRIES OF FLORIDA IT COUNCIL
McCONNAUGHHAY · COONROD POPE · WEAVER · STERN P.A.
FLORIDA ECONOMIC DEVELOPMENT COUNCIL EDUCATE. ADVOCATE. CONNECT.
ASSURITY DRIVE
CYBER FLORIDA at the UNIVERSITY OF SOUTH FLORIDA
TBDA TAMPA BAY DEFENSE ALLIANCE
ENTERPRISE FLORIDA
FDCA FLORIDA DEFENSE CONTRACTORS ASSOCIATION
Florida State Hispanic Chamber of Commerce
THE NATIONAL CENTER FOR SIMULATION
THE FLORIDA COUNCIL OF 100
SPACE FOUNDATION
Florida Trend FLORIDA'S BUSINESS AUTHORITY
COMCAST BUSINESS
florida internet & television
bmc AMI
GOLDSKY CYBER SECURITY SOLUTIONS
FLORIDA DEFENSE SUPPORT TASK FORCE
SPACE FLORIDA
CENTER FOR CYBERSECURITY AT THE UNIVERSITY OF WEST FLORIDA
PORT TAMPA BAY
SecureStrux
UCF
www.glesec.com GLESEC
THE Florida COLLEGE SYSTEM FOUNDATION
GROWFL TAKING SUCCESSFUL COMPANIES TO THE NEXT LEVEL
AVT Simulation
ivanti

Sponsorship Opportunities

Sponsorship Levels

Title Sponsor – $20,000

- Option to present company promotional video during the virtual Forum
- Featured article on WCI website and in the Forum materials
- One-time promotional ad of noting as Title Sponsor pushed out through social media
- Ability to participate in the event program as a panelist or introduce a VIP speaker
- Set up a virtual exhibit space (Premier level provided) to gain interest and speak with potential clients via a chat room
- Option to include a promo ad with link to your company's virtual exhibit during the virtual Forum sessions and in the Forum materials
- Unlimited complimentary registrations to share within your organization and clients
- Comprehensive attendee contact list provided for future reference
- Company logo on materials, virtual signage, website and promotional emails
- Verbal acknowledgment during the Forum

Gold Sponsor – $10,000

- Ability to participate in the event program as a panelist or introduce a VIP speaker
- Set up a virtual exhibit space (Premier level provided) to gain interest and speak with potential clients via a chat room
- Option to include a promo ad with link to your company's virtual exhibit during the virtual Forum and in the Forum materials
- Unlimited complimentary registrations to share within your organization and clients
- Comprehensive attendee contact list provided for future reference
- Company logo on materials, virtual signage and website
- Verbal acknowledgment during the Forum

Silver Sponsor – $5,000

- Set up a virtual exhibit space (Professional level provided) to gain interest and speak with potential clients via a chat room
- Option to include a promo ad with link to your company's website in the Forum materials
- Unlimited complimentary registrations to share within your organization and clients
- Company logo on materials, virtual signage and website
- Verbal acknowledgment during the Forum

Bronze Sponsor – $3,000

- Set up a virtual exhibit space (Professional level provided) to gain interest and speak with potential clients via a chat room
- Option to include a promo ad with link to your company's website in the Forum materials
- Eight complimentary registrations to share within your organization
- Company logo on materials, virtual signage and website
- Verbal acknowledgment during the Forum

Virtual Exhibitor – Prices starting at $500

- Set up a virtual exhibit space to gain interest and speak with potential clients (exhibitor levels range from Premier to Classic, with varying prices)
- Four complimentary registrations to share within your organization
- Company name listed as a virtual exhibitor on materials, virtual signage and website

Please contact Cathy Bowman at cathy@wci360.com for more information or to sponsor this event.
Register at www.wci360.com/cyber.

Registration Form

Name

Company Name | Title

Industry | Are you a defense contractor? Yes / No | About how many employees work at your company?

Business Mailing Address

City | County | State | ZIP

Telephone Number | Fax Number | Email Address

REGISTRATION:

❑ I have enclosed a check; or authorize WCI to charge $49 to my credit card.

SPONSORSHIPS:

Please Select Sponsorship Type:

❑ Title Sponsor I have enclosed a check; or authorize WCI to charge $20,000 to my credit card.
❑ Gold Sponsor I have enclosed a check; or authorize WCI to charge $10,000 to my credit card.
❑ Silver Sponsor I have enclosed a check; or authorize WCI to charge $5,000 to my credit card.
❑ Bronze Sponsor I have enclosed a check; or authorize WCI to charge $3,000 to my credit card.
❑ Virtual Exhibitor I have enclosed a check; or authorize WCI to charge $500 to my credit card.

METHOD OF PAYMENT: ❑ Check ❑ Mastercard ❑ VISA ❑ American Express ❑ Discover

Credit Card Account Number | Expiration Date | CVV | Signature

❑Check here if you have special needs that require attention.

SEMINAR FEE: $49.00

MAKE CHECKS PAYABLE TO:
Workers' Compensation Institute, Inc.
FEIN # 59-2846608

MAIL TO: Workers' Compensation Institute, Inc.
P.O. Box 200
Tallahassee, FL 32302-0200

OR FAX TO: (850) 521-0222 (Mastercard/Visa/AmX/Discover)

OR REGISTER ONLINE AT: WWW.WCI360.COM/CYBER

REGISTRATION: Mail the completed registration form, along with credit card information (VISA/MC/AmX/Discover) or a check made payable to: Workers' Compensation Institute, Inc., P.O. Box 200, Tallahassee, Florida 32302-0200; or fax form to (850) 521-0222; or register online at www.wci360.com/cyber.

The forum is from 8:45 a.m. to 5:00 p.m. on Wednesday, and 8:00 a.m. to 3:00 p.m. on Thursday. Cost is $49.00. For more information, contact the Workers' Compensation Institute at (850) 425-8156 or 425-8155. REGISTRATION IS REQUIRED TO ATTEND.

REFUND POLICY: Cancellations must be made more than 7 days prior to the seminar. A processing fee will be charged on all cancellation requests postmarked 7 days prior to the seminar date. Registrants who do not cancel and do not attend the seminar are liable for the entire fee. Refunds will be processed within 30 days following seminar.

SPONSORSHIPS: Sponsors must complete registration form with selected sponsorship and return to WCI.

Direct inquiries regarding continuing education to WCI – (850) 425-8156.