



CYBER USA

**Tuesday,
January 30, 2018**

**Henry B. Gonzalez
Convention Center**

San Antonio, TX





WELCOME TO SAN ANTONIO

Welcome to the inaugural CyberUSA Conference 2018. This one day event will bring the cyber community together to collaborate on the mission purpose of establishing innovation, education, workforce development, enhanced cyber readiness, and resilience. This conference is a gathering of current and future CyberUSA affiliates which is made up of academia, government, industry, and students.

JOIN THE NATIONAL COMMUNITY

Become part of the national network of cyber states. If you represent a technology council, chamber of commerce, cyber group, ISAO, ISAC, or other Trust-based membership group, we invite you to register and bring your group into the 'community of communities' to begin sharing, being shared with, and together we can secure the nation!



CONNECTING TRUST COMMUNITIES

Innovation • Education • Workforce • Communication

CyberUSA

CyberUSA is a collaboration of states focus on a common mission purpose of enabling innovation, education, workforce development, enhanced cyber readiness and resilience – all while connecting the cyber ecosystem of the United States and its Allies. This non-profit “community of communities” is governed by its members, established to enhance information sharing between states and improve cyber resilience at all levels of participation – local, regional, and national. CyberUSA provides a communication framework, a national summit and cyber related resources to communities across the United States.

Engagement

Individual CyberUSA Affiliate Communities work together as Information Sharing groups, leveraging tools, best practices and a platform for maintaining trust and a vetted membership. Engaging where they serve, CyberUSA affiliates create more resilient local communities, marketplace opportunities, shared awareness and solutions. This helps make our communities safer throughout the United States.



SALUTE THE PAST... EMBRACE THE HORIZON

SAN ANTONIO CYBER HALL OF HONOR AWARD CEREMONY

MONDAY
JANUARY

29

HENRY B. GONZALEZ CONVENTION CENTER

CEREMONY 5:00PM – 5:30PM

RECEPTION 5:30PM – 7:00PM

2017 INDUCTEES

**MR. ROBERT
J. KAUFMAN**

**MR. FRED
M. RAMIREZ**

**MR. DWAYNE
WILLIAMS**

JOIN US IN HONORING OUR INDUCTEES INTO THE CYBER HALL OF HONOR

VISIT OUR WEBSITE FOR MORE INFORMATION

WWW.FBCINC.COM/CYBERUSA



Monday, January 29, 2018

Time	Agenda Item
5:00 PM – 7:00 PM	San Antonio Hall of Honor Reception in Room 301

Tuesday, January 30, 2018

***All Sessions will take place in Room 301. The Exhibit Hall is located in Room 302 AB.**

Time	Agenda Item
7:30 AM - 11:00 AM	Registration
8:00 AM – 8:15 AM	San Antonio Welcome <i>Judge Nelson Wolff, Bexar County</i>
8:15 AM – 8:30 AM	CyberUSA Introduction <i>The Honorable Philip J. Bond, Co-founder & Executive Director, CyberUSA</i> <i>David Powell, COO, FBC; Co-Founder & Vice Chair, CyberUSA</i>
8:20 AM – 8:50 AM	Morning Keynote Government Cyber Opportunities for your Region: The Federal Agenda – Federal Funding, Grants & Resources Available to support Community Cyber Initiatives <i>John W. Lainhart, Director – Cybersecurity Executive, grant Thornton LLP</i>
9:00 AM – 2:00 PM	Exhibit Hall Opens
9:00 AM – 9:15 AM	DHS Update <i>George Reeves</i>
9:15 AM – 9:45 AM	Networking Break
9:45 AM – 10:15 AM	Cyber Education Session Using Automation to Enhance Cyber Workforce Development <i>Michael Cameron, Noblis NSP</i>
10:15 AM – 10:50 AM	Cyber Education Session Filling the Gap – Exploring New Advancements in Cybersecurity Education Programs Moderator: <i>Dr. Loyce Best Pailen, CISSP Director, Center for Security Studies, UMUC</i> Panelists: <i>Akhtar Lodgher, Computer & Cybersecurity, Texas A&M University</i> <i>Laurin Buchanan, Secure Decisions</i> <i>Frank Downs, Senior Manager of Cyber Information Security Practices, ISACA</i>
10:50 AM – 11:15 AM	Cyber Education Session Using Cyber competitions to Develop the Cyber Workforce <i>Bernie Skoch, CyberPatriot National Commissioner, The Air Force Association</i>
11:15 AM – 11:35 AM	TruSTAR and CyberUSA <i>Paul Kurtz, TruSTAR Technology</i>

Tuesday, January 30, 2018 Continued

Time	Agenda Item
11:35 AM – 12:00 PM	<p>Cyber Workforce Development Session Building a Community of Women in cybersecurity / Filling Jobs That Do Not Yet Exist <i>Moderator:</i> Princess Young, Program Manager, Cybersecurity Awareness, Office of Cybersecurity & Communications, U.S. Department of Homeland Security</p>
12:10 PM – 12:20 PM	Networking Break
12:20 PM – 1:00 PM	<p>Lunch Keynote The Impact of Information Sharing – The Emerging Information Sharing Ecosystem Dr. Greg White, Director, Center for Infrastructure Assurance and Security, The University of Texas at San Antonio</p>
1:00 PM – 1:35 PM	<p>Cyber Capacity Building Session Bringing Cyber Market-Making to Main Street USA Doug DePeppe, Cyber Resilience Institute (CRI) Jane Ginn, Cyber Resilience Institute</p>
1:40 PM – 2:05 PM	<p>Capacity Building General Session <i>Moderator: Jennifer Sabas</i>, CyberHawaii <i>Panelists:</i> Dennis Gibson, Senior Vice President, Booz Allen Hamilton Amy Aapala, Vice President, Information Technology Systems & Order Management Systems, Hawaiian Telcom Steve Auerbach, Director, Pacific Center for Advanced Technology Training (PCATT) at Honolulu Community College</p>
2:05 PM – 2:40 PM	<p>Cyber Innovation Session The Top 5 Cyber Threats to Your Region & How to Work Together for Prevention & Remediation <i>Moderator: Anne Townsend</i>, NIST – NCCoE <i>Panelists:</i> Andre Dempsey, Def-Logix, Inc. Ethan Schmertzler, Dispel Pierluigi Stella, Network Box USA, Inc.</p>
2:45 PM – 3:05 PM	<p>Cyber Innovation Session CyberUSA and Protecting America’s Elections Andy Liverman, Dispel & Don’t Hack the Vote</p>
3:05 PM – 3:15 PM	Networking Break
3:15 PM – 4:00 PM	<p>Cyber Information Sharing Session The Importance of Information Sharing in Protecting Your Community Ian Schmertzler, Dispel Renault Ross, CISSP, MCSE, CHSS, CCSK, CISM, Chief Cybersecurity Business Strategist, Symantec Americas Strategic Programs</p>
4:00 PM – 4:25 PM	<p>Closing Remarks Joe Sanchez, Founder, CyberTexas</p>

ABSTRACTS

Morning Keynote: *Government Cyber Opportunities for your Region: The Federal Agenda - Federal Funding, Grants & Resources Available to Support Community Cyber Initiatives*

Speaker: John Lainhart, Principal, Grant Thornton Cyber Executive

Abstract: The influx of government spending on cybersecurity generates immense opportunity for commercial IT companies and cyber workforces. The acquisition and deployment of existing and emerging technologies coupled with the training of a robust cyber workforce strategically positions the government's national security interests. Learn about the USG's cybersecurity needs, the approach to R&D, and the procurement of new innovative solutions to some of the nation's toughest cybersecurity challenges. Gain insights into upcoming cybersecurity projects and potential opportunities for collaboration and funding. Hear from practitioners on best practices to build sustainable relationships with federal departments and agencies.

Cyber Education Session: *Using Automation to Enhance Cyber Workforce Development*

Speaker: Michael Cameron, *Noblis, NSP*

Abstract: Conventional measures of the cyber workforce have focused on the number of individuals in the workforce and their level of training. Headcount and training are easily measurable properties of the workforce, but they serve mainly to quantify the growing gap between the workforce we have and the workforce we need for a rapidly expanding cyber mission. Thinking in terms of "mission gap" rather than headcount and training gaps suggests a different way of looking at workforce development. While trying to close the gap by hiring and training greater numbers of people, it's also important to look at the contribution technology can make to workforce development by making each person in the workforce more effective. Properly designed tools that enable greater productivity, combined with robust recruiting and training, can close the mission gap much faster.

Cyber Education Panel Session: *Filling the Gap – Exploring new advancements in cybersecurity education programs*

Moderator: Loyce Pailen, Director of Cybersecurity Studies, University of Maryland University of College.

Panel Member:

Akhtar Lodgher, Computing & Cybersecurity, Texas A&M University

Laurin Buchanan, Secure Decisions

Frank Downs, Senior Manager of Cyber Information Security Practices, ISACA

Abstract: The demand for cybersecurity talent is expected to rise to six million globally by 2019. This year alone, one million cyber jobs are opening and over 200,000 jobs in the U.S. are unfilled. The case has been made for why cyber education and workforce development are high-stake missions in the fight against cyber-crime. Learn why a thriving U.S. cyber workforce is at the helm of effective STEM initiatives, college, university curriculum development, cyber training, and alternative education methods for preparing our nation's heavily sought-after cyber leaders.

Topic Discussions

- Beyond Commands & Code – Understanding Choices
- Holistic Approach to Teaching Cybersecurity



Cyber Education Session: Using Cyber Competitions to Develop the Cyber Workforce

Speaker: Bernie Skoch, Air Force Association

Abstract: The U.S. is not attracting enough young people to science, technology, engineering and mathematics. The Air Force Association's CyberPatriot -- National Youth Cyber Education Program -- excites, educates, and motivates the next generation of cyber defenders, raises public awareness, and promotes safer practices among cyber users across the nation. The program features the National Youth Cyber Defense Competition for high school and middle school students, AFA Cyber Camps, and an Elementary School Cyber Education Initiative.

This presentation will provide an overview of the program's accomplishments, and how it has positively shaped cyber education in elementary, middle and high schools across the nation, in Canada, and in other friendly nations worldwide.

Cyber Science, Analytics & Threat Intelligence Session: Using & Leveraging Threat Intelligence to Support Cyber Sharing Communities

Speaker: Paul Kurtz, CEO, TruSTAR

Abstract: Understanding sophisticated cyber adversaries, specifically how they threaten government and industry assets, help network protectors make informed decisions. The science behind cybersecurity strategies allow experts to build a blueprint for how to identify, conceptualize, and defend against malicious malefactors. Learn how threat intelligence is used, and misused, to guard critical data and what cyber science and data analytics. In the gloomiest shadows of the cyber world, an enemy has been permitted to grow and gain momentum. Communities are banding together across the country under the CyberUSA banner, building their own cyber-state organizations to combat the cyber threat. Shared 'indicators of compromise' and potential remediation strategies are crucial to staying ahead of the bad guys. This session will discuss best practices for launching a threat sharing and incident intelligence network within your cyber community.

Cyber Workforce Development Session: Building a Community of Women in Cybersecurity / Filling Jobs That Do Not Yet Exist

Moderator: Princess Young, Department of Homeland Security, Cybersecurity Education and Awareness

Abstract: How can public, and private organizations work together to bring more cybersecurity education and employment opportunities to women in their local communities and nationwide. While cybersecurity jobs are at an all-time high, the gender gap in the field of cybersecurity remains wide. It takes a coordinated effort from government, schools, and the community to build awareness and interest in cyber careers among women of all ages, no matter if they are in a small town or in the nation's capital. This session will bring together female cybersecurity professionals as well as advocates for women in cybersecurity to share how they became interested in cyber and what opportunities led to their current careers. Additionally, this panel will discuss the ways public and private organizations can work together to increase opportunities for women in cybersecurity at the local, regional and national level.

Cyber Information Sharing Session: The Impact of Information Sharing -The Emerging Information Sharing Ecosystem

Speaker: Dr. Greg White, University of Texas San Antonio & ISAO Standards Organization

Abstract: Cybersecurity Information Sharing and Analysis is obviously not a new topic but with the publication of Executive Order 13691 the creation of a much larger information sharing ecosystem has begun. Initial guidance from DHS described a future environment with potentially 1000's of Information Sharing and Analysis Organizations (ISAOs). What will this emerging ecosystem look like and how will these 1000's of ISAOs work together with already existing information sharing and analysis organizations to build a robust and cooperative ecosystem? This talk will begin with a general discussion of the importance and benefit of an information sharing and analysis program for both government and industry sectors. It will then discuss the current state of the information sharing ecosystem and the emerging standards and guidelines, what is being developed and how can everybody work together. It will finish with a brief examination of what the future of the ecosystem may hold.



Cyber Capacity Building Session: Bringing Cyber Market-Making to Main Street USA

Speaker: Douglas DePeppe & Jane Ginn, Cyber Resilience Institute

Abstract: What if building cyber resilience could be a community economic driver? If market forces behind cyber solutions could revitalize Main Street? If a rising tide of cyber markets could lift the boats of small and mid-size businesses in a community? And what if a market-based approach to security could return global competitiveness to Western democracies through free market economics? The Cyber Market Development Project, a DHS-funded effort under the NIPP Security and Resilience Challenge, has revealed a Community Cyber Marketplace model – c-Market™. This talk will introduce cyber market-making and c-Market™, along with the rollout of community capacity building activities throughout 2018 to help stand-up Community Cyber market-making. c-Market™ is a complementary and partnered offering with CyberUSA. From this talk, attendees will learn what Community Cyber, market-making, and how to become a community champion.

Capacity Building General Session

Speaker: Jen Sabas, CyberHawaii

Abstract: Ms. Jennifer Sabas and her team have been instrumental in building the information sharing and analysis non-profit organization (ISAO) now known as CyberHawaii, committed to developing and enhancing Hawaii's cybersecurity capabilities. CyberHawaii also develops and accelerates the educational opportunities for students via pathways from high school to two and four year cyber degrees. This includes early college credits to incentivize a running start to college and then the workplace. Ms. Sabas will discuss the process of standing up the organization, how this was accomplished and lessons learned.

About Jennifer Sabas: Ms. Sabas also holds the position as Director of the Daniel K. Inouye Institute Fund, Executive Director of Move Oahu Forward, Consultant to Military Affairs Council at the Chamber of Commerce Hawaii, and Washington Consultant for the University of Hawaii (UH). From January 1993 to February 2013, she was Chief of Staff for the late U.S. Senator Daniel K. Inouye's Hawaii and Washington, DC offices. Under Senator Inouye, Ms. Sabas managed the staff, legislative agendas on all areas important to Hawaii, and was a political confidant to the Senator, serving as campaign and political lead in Washington, DC and Hawaii.



Cyber Innovation Session: The Top 5 Cyber Threats to Your Region & How to Work Together for Prevention & Remediation

Moderator: Anne Townsend, NIST, NCCoE

Panel Members:

Andre Dempsey, Def-Logix, Inc.

Ethan Schmertzler, Dispel

Pierluigi Stella, Network Box USA, Inc

Abstract: Ransomware, malware, malicious insiders, and human mistake constantly jeopardize data integrity for any organization regardless of size or industry. The consequences of these attacks not only impact the data but they are costly for both operations and reputation. From discussions that began with the Financial Services Information Sharing & Analysis Center (FS-ISAC) and their Destructive Malware Task Force, we learned that developing a methodology to recover from these events can be difficult for organizations. This session will discuss how industry experts and technology collaborators worked with the National Cybersecurity Center of Excellence (NCCoE) to develop practical cybersecurity guidance on recovering from destructive malware & ransomware. The session will highlight the recently released NIST Special Publication 1800-11, Data Integrity: Recovering from Ransomware and Other Destructive Events, and how a company can implement the solution to efficiently recover from data integrity.

Topic Discussions:

- Weathering the Cloud & its Security Implications (The cloud is no longer something for the future)
- Bad Bait, Gone Phishing – accommodating for human error
- An ounce of prevention is worth a bitcoin of cure – taking a proactive approach to cyber-attacks and risks.

Cyber Innovation Session: CyberUSA and Protecting America's Elections

Speaker: Andy Liverman, Dispel

Abstract: This session will cover the basic challenges and offer solutions for securing our elections from the well-publicized issues with voting machines, to the less known threats to the voting rolls, and vote tallying process. A cornerstone of our democracy, the electoral process is under cyber-attack from foreign adversaries. State and local electoral officials are out matched and inexperienced in how to adequately protect themselves. While the federal government has offered some assistance, ultimate control of the election systems resides in local hands, and many of these local officials are reluctant to accept assistance from federal authorities. The cybersecurity community and CyberUSA can play a key role in helping to secure the election process from cyber-attacks. Our members, from experienced professionals to students, need to join together to provide guidance, assistance, and on-the-ground support to the local officials and the thousands of election sites around the country.

Cyber Information Sharing Session: The Importance of Information Sharing in Protecting Your Community

Speakers: Ian Schmertzler, Dispel and Renault Ross, Symantec

Abstract: This is a presentation about supply chains, cyber security, and communicating with industry. While it is far safer to procure products whose software is written, and hardware manufactured, entirely within the borders of America and her closest allies by the citizens thereof, it is often hard for civilian governments to find sophisticated products fitting that description.

What is there to be done? First, we will cheer you up by showing you clouds that fly; swarms; cloaked comms; and a few other pieces of tech that are made in the USA. We will then tell some tales of our experiences enforcing supply chain discipline in the commercial sector and explain, as best as we can, the concerns that have kept some of the key advanced providers out of the civilian government space.

A recent NASCIO pool ranked security and risk management as the top state CIO priority. It was the same the year before and will likely be the same next year. The reasoning is simple: like their colleagues in the federal government – not to mention the private, education and healthcare sectors – nothing is more important than information security. And, when it comes to sharing information between state agencies and the partners noted above, the security requirements magnify. This session will outline how the best approach to secure information sharing starts with the data. It will provide insights and best practices on how to establish data access control no matter who is accessing it or where it resides. Specific areas of focus include:

- Defining what level of access a user has through digital rights management technology
- Monitoring user access to sensitive data to identify risky behavior
- Revoking access to users to effectively digitally shred a document



CYBERSECURITY. AT SCALE. WITH SPEED.

Combining tradecraft and technologies to create
force multipliers for critical cyber missions

JOIN US. GET HIRED.

CYBER SECURITY PROFESSIONALS CHECK OUT OUR
SITES TO FIND YOUR NEXT CAREER OPPORTUNITY

EMPLOYERS CONTACT US ABOUT HOW YOU CAN
CONNECT WITH TOP CYBER TALENT

TAKE ADVANTAGE OF OUR RESOURCES FOR A SUCCESSFUL 2018!

— 2018 — SAN ANTONIO JOB FAIRS

APRIL 19
CYBER JOB FAIR
MARRIOTT COURTYARD

AUGUST 14
CYBERTEXAS JOB FAIR
HENRY B. GONZALEZ
CONVENTION CENTER

NOVEMBER 15
CYBER JOB FAIR
MARRIOTT COURTYARD

PROUD JOB FAIR PARTNERS OF CYBERMARYLAND
AND CYBERTEXAS SINCE 2014



CYBERSECJOBS
www.cybersecjobs.com

ClearedJobs 
www.clearedjobs.net

ArnoldIT

Stephen E. Arnold
7202 Iron Gate Court
Louisville, KY 40241
(502) 228-3820
sa@arnoldit.com
<http://www.xenky.com>



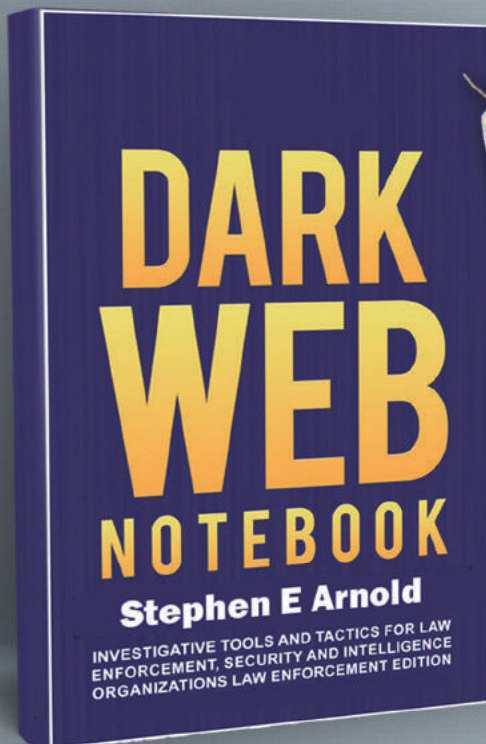
Stephen E Arnold is a semi-retired indecent "analyst." He provides strategic information services to clients worldwide. He is the author of CyberOSINT: Next Generation Information Access and Dark Web Notebook. He produces a weekly LE and intelligence oriented news video called Dark Cyber. Videos are available from www.arnoldit.com/wordpress, YouTube, and Vimeo.

Non-Exhibiting Event Sponsor

Ciena

Ronald Jones
7031 Ridge Road
Hanover, MD 21076
(301) 204-1999
rojones@ciena.com
<http://www.ciena.com>
Telecommunications Equipment Manufacturer, Software Defined Networking.

THE DARK WEB NOTEBOOK: LE AND INTEL EDITION



Order The PDF Online at



Immediate download
after payment

What's in the Dark Web Notebook

1	Why the Dark Web is important
2	Dark Web Q&A
3	A revealing Dark Web tour
4	Basic investigation safeguards
5	Advanced investigation safeguards
6	How to research the Dark Web using the Surface Web: Pastesites, Reddit, and more
7	Hacking the Dark Web with open source (free) software
8	Commercial Dark Web services
9	Bitcoin and digital currencies
10	Privacy issues
11	What's ahead for investigators
12	A glossary for investigators
13	The Defense Advanced Research Agency Dark Web software: A list with download locations
14	Detailed table of contents
15	Comprehensive index

This June 2017 book is in plain English, with key concepts illustrated with screenshots, diagrams, and original illustrations.



CyberTexas Foundation

Adam Cavazos
425 Soledad
Suite 600
San Antonio, TX 78205
(210) 355-5642
acarazos@cybertexas.org
<https://www.cybertexas.org>

The National Initiative for Cybersecurity Careers and Studies (NICCS) is the premier online resource for cybersecurity training. NICCS connects Government employees, students, educators, and industry with cybersecurity training providers throughout the Nation. Providers include accredited universities, National Centers of Academic Excellence, federal agencies, and cybersecurity training providers.

Learn More: <https://niccs.us-cert.gov>

NETSCOUT Systems, Inc.

Steve Pearring
310 Littleton Road
Westford, MA 01886
(978) 320-2159
Stephen.Pearing@netscout.com
<http://www.netscout.com>



NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) is a market leader in real-time service assurance and cybersecurity solutions for today's most demanding service provider, enterprise and government networks. NETSCOUT's Adaptive Service Intelligence™ (ASI) technology continuously monitors the service delivery environment to identify performance issues and provides insight into network-based security threats, helping teams to quickly resolve issues that can cause business disruptions, impact user experience or threaten mission success. www.netscout.com



nGeniusONE SERVICE ASSURANCE PLATFORM

GAIN HOLISTIC VIEW OF SERVICE
DELIVERY INFRASTRUCTURE

ASSURE HIGH QUALITY
USER EXPERIENCE

DRASTICALLY REDUCE CAPEX AND
OPEX COSTS

BREAK DOWN OPERATIONAL AND
TOOL-BASED SILOS

NETSCOUT®

Guardians of the Connected World

www.netscout.com



Network Box USA

Kevin Brown
2825 Wilcrest Drive
Suite 259
Houston, TX 77042
(832) 242-5758
kevin.brown@networkboxusa.com
<http://www.networkboxusa.com>

Network Box USA is a leading MSSP in the US, providing exceptional and affordable enterprise-level security solutions. We have three ISO certifications (ISO 9001, 20000, 27001), various Global Security Operation Centers (SOCs) in the US, Europe, Middle East, Asia and Australia, and a dedicated Security Response Center (SRC). Since 2000, we have served thousands of businesses around the world, across multiple sectors, with state-of-the-art cyber security solutions built upon our proprietary, comprehensive, real-time technology. A technology which has, to date, garnered over 100 international awards.

Noblis/Noblis NSP

Mike Cameron
Noblis HQ: 2002 Edmund Halley Drive
Reston, VA 20191
Noblis NSP: 2721 Technology Drive, Suite 400
Annapolis Junction, MD 20701
(301) 479-3055
Michael.Cameron@noblis-nsp.com
<http://www.noblis.org>



Noblis and Noblis NSP combine cyber operations, research, machine intelligence, and data analytics expertise to provide value for our customers. We leverage lessons learned, subject matter expertise, and cutting edge tools to develop actionable, and responsive processes for our clients. Our solutions meet unique needs in ways off-the-shelf products cannot.

Non Exhibiting Morning Break Sponsor

VT Miltope

JB Curtis
3800 Richardson Road South
Hope Hull, AL 36043
(334) 613-6377
jcurtis@miltope.com
<http://www.mymiltope.com>



VT Miltope serves defense, government, and commercial markets with a broad range of rugged computers, workstations, servers, and other peripheral computing systems. VT Miltope is ISO 9001/AS 9100 certified and designs, develops, manufactures, and tests its products to ensure reliable operation in demanding environmental operating conditions.



Are you tasked with planning a Cybersecurity Training Event or Workshop for your agency?

Then We're Your Answer! The Federal Business Council has established a proven track record of accomplishments in coordinating Cybersecurity Events. We are experienced on every level in diverse topic areas covering not only education and informational symposiums, but also workshops, exhibits, seminars, themed presentations, and training forums in the federal area.



The Federal Business Council (FBC) is a professional organization providing meeting and conference support for the DoD, Intelligence Community, and Federal Civilian Agencies since 1976.

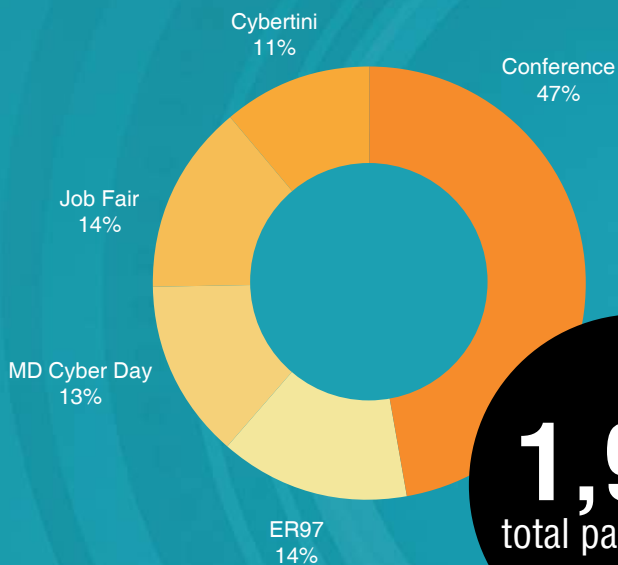
For questions about exhibit opportunities, please call us at (800) 878-2940 ext 283 or email bj@fbcinc.com.
To view a list of our current events, please visit our website at www.fbcinc.com.

SAVE THE DATE

CYBER•MARYLAND2018

October 9 & 10, 2018 | The Hyatt Regency Baltimore Inner Harbor

Academia, entrepreneurs, innovators, government, students, and CyberUSA members will join together in Maryland, the nation's epicenter for cybersecurity, for the eighth annual CyberMaryland Conference.



1,957
total participation

- Over 1,000 attendees from academia, government, and industry sectors
- Over 70 exhibitors and sponsors
- With 25 tracks featuring keynote speakers, panelists, and moderators
- Topics discussing the primary 4 topics—Education, Workforce Development, Innovation, and Communication
- Cyber Job Fair—For cleared and non-cleared cybersecurity professionals



www.fbcinc.com