



Welcome to 2021!"

I know we are holding our breath in anticipation of a better year to come but, come what may, rest assured our chapter is ready to attack it head-on. We are excited for the year ahead and the opportunity to return to many of our traditional core events while also incorporating new capabilities adopted from our experiences in 2020. Despite the challenges we all faced in 2020, the year proved be quite successful for our chapter. In this article, we will take time to pay tribute to the people and events that made 2020 such a success then, we will shift gears and preview the core events on tap for 2021. Buckle up folks... the fun is about to begin!

In 2020, the year started out much like any other; with a renewed anticipation of great events to come. In January and February, we enjoyed a strong start to the monthly chapter meetings and mini seminars. As we moved into March, we were super excited about our upcoming Cyber Focus Symposium; then, COVID hit. With less than two weeks to go before the symposium, we made the difficult decision to cancel the event. The next few days were very telling as the full impact of COVID began to set in. Across the Colorado Springs

region, businesses were shifting to a work-from-home model, grocery stores began rationing cleaning supplies and personal sundry items, and personal service businesses such as hair salons, nail salons, and barbershops were forced to shutter their doors. As for our chapter, the need to indefinitely cancel our in-person events became a reality. It appeared dark days were upon us.

For many chapters across ISSA, the effects of COVID forced them to suspend operations. Even ISSA itself was forced to cancel their annual conference. For ISSA-COS however, we rose to the challenge and in less than ten days, our IT Committee successfully adopted a fully virtual platform, and our Speakers Bureau Committee developed a series of online presentations. Within the first week of April, we were back in operation providing quality content for both our chapter members and our community at large.

Highlights from throughout the year included:

- Presentations from 39 different guest

(Continued on page 4)

A Note From Our President

By Mr. Ernest Campos

The ISSA Colorado Springs Newsletter incorporates open source news articles in compliance with USC Title 17, Section 107, Paragraph a (slightly truncated to avoid copyright infringement) as a training method to educate readers on security matters .

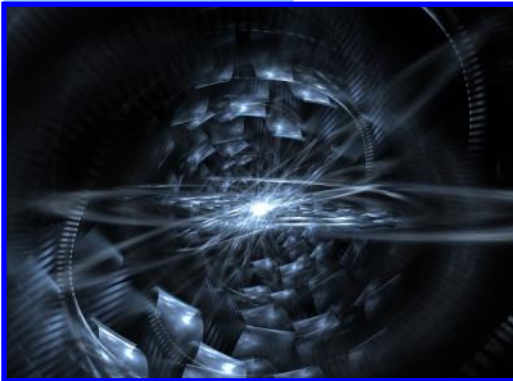
The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our members, and do not constitute or imply endorsement by ISSA or the Colorado Springs Chapter of ISSA of any entity, event, product, service, or enterprise.

The Pentagon is ill-organized to improve its use of electromagnetic spectrum, GAO says

By Staff, American Military News, December 22, 2020

The U.S. military has big plans for better harnessing the electromagnetic spectrum, but lacks the organizational setup to do it, says the Government Accountability Office, or GAO. The department hasn't even figured out who should be in charge of implementing its months-old strategy, let alone how to connect or combine the service's many related projects and efforts.



"DOD officials from multiple offices with [electromagnetic spectrum] duties identified a lack of central coordinating authority as a major

challenge to effective EMS governance," says the report, issued on Thursday. "An official from the [cross-functional team] said that EMS-related duties are spread across the department and there is a need for a DOD official that can be held responsible for EMS issues."

The problem isn't so much a lack of high-ranking defense officials with eyes on electronic warfare and spectrum issues. It's that those people have a lot of other important things to do, so while they may all agree that spectrum warfare is critical and that the Defense Department should follow its own strategy, they're also in charge of things like nuclear deterrence or fixing the Defense Department's information technology infrastructure. So spectrum issues become everybody's second job.

"Senior-level DOD officials responsible for department-wide EMS management are assigned many non-EMS-related responsibilities. For example, the Vice Chairman of the Joint Chiefs of Staff, a four-star general officer, is DOD's Senior Designated Official for the [cross-functional team] but has numerous other responsibilities," notes the report. "Those who focus on EMS-related issues full-time are most often located at lower organizational levels within DOD."

Some of the hardware that the Defense Department is using remains "fundamentally unchanged in design since they were fielded decades ago," which, in addition to being obsolete, aren't interoperable with newer pieces of equipment or allied hardware.

Overly bureaucratic buying practices are another obstacle, the report said.

It comes at a time when the Defense Department is changing how it approaches electromagnetic warfare.

For instance, the Department is developing electronic warfare teams called Joint Electromagnetic Spectrum Operations Cells, or JIMSOCs, which the Department hopes to embed with combatant commands. These cells will use a new planning-and-situational awareness tool, dubbed Electromagnetic Battle Management, being developed by U.S. Strategic Command and the Defense Information Services Agency. "We are using a rapid software acquisition process to acquire" the tool, STRATCOM'S Brig. Gen. AnnMarie Anthony said Thursday during a Mitchell Institute webinar.

Spectrum warfare tools have changed dramatically in recent years, with innovation moving away from hardware toward software-defined radio whose code-based mixers and detectors can quickly adjust and shift between frequencies. That makes it easier to purchase EO hardware that can perform more than one function, which is changing the way the Defense Department buys that equipment, said David Tremper, who directs electronic warfare at the Office of the Secretary of Defense. "Different services are taking that multi-function approach. There's an acquisition impact we have to assess. We are taking a close look at that," Tremper said in the webinar.

The emergence of software-defined networking and new digital spectrum tools, if the Department and operators can embrace them, will do much to address issues like interoperability and slow acquisition, since software can always be reprogrammed to suit different needs.

Read the rest here:

<https://americanmilitarynews.com/2020/12/the-pentagon-is-ill-organized-to-improve-its-use-of-electromagnetic-spectrum-gao-says/>

"It comes at a time when the Defense Department is changing how it approaches electromagnetic warfare."





Membership Update

Have you updated your contact information on the ISSA International website? You have! That is awesome. If you have not, please log onto the ISSA International website and click on your welcome icon on the top of the page and select "Account + Settings". Once there you can make your updates. Thank you for your support.

We need all members to spread the word that we are looking for new members to join our great organization. Below are the top 10 reasons join ISSA!

Top 10 Reasons Cybersecurity Professionals Join ISSA

1. Build professional relationships
2. Learn practical/best practices solutions
3. Keep up on developments in information security/risk/ privacy
4. Career information and employment opportunities
5. Content of chapter meetings
6. Advance the profession
7. Professional development or educational programming offerings
8. Give back to the profession
9. Earn CPEs/CPUs
10. Develop the next generation of cybersecurity professionals

Our membership is hanging in at ~329 members as of the end of December 2020. Please watch the newsletter, communications and eVites to ensure you stay aware of what's going on in the chapter. As always, if you have any membership questions don't hesitate to contact me.

Thanks,

Steven Mulig

VP-Membership

membership@issa-cos.org

New Members December

Nicholas A. Cameron

Trent Brantt Bunnell, Sr.

Google confirms it notifies children if parents are monitoring their accounts

By Daniel Payne, Just The News, December 21, 2020

Google informs children when their parents are monitoring their account activity, the tech giant confirmed this month, with the company claiming that doing so is a way of balancing the interests of both parents and children.

Google's child-notification policies received attention when film director Robby Starbuck claimed on Twitter that his 7-year-old child had received a warning from Google that his account was being monitored.

"Our 7-year-old son has to have google for homeschooling," Starbuck wrote on Twitter, "so naturally we setup parental controls but look what [Google] did. They sent my son an email to tell him his privacy is important to them and telling him we're supervising his account."

"Your privacy is important to us," the company wrote to the 7-year-old boy, "and we want to remind you that your parent ... is supervising your Google account."

Company cites United Nations declaration on child privacy rights

Reached for comment, the company confirmed it does notify young children when parents are monitoring their account activity.

The company pointed to both the UN Convention on the Rights of the Child and the recently passed UK Age Appropriate Design Code as examples of child-privacy advocacy to which it adheres.

The UN Convention on the Rights of the Child—which dates to September 1990— holds, in part, that "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation."

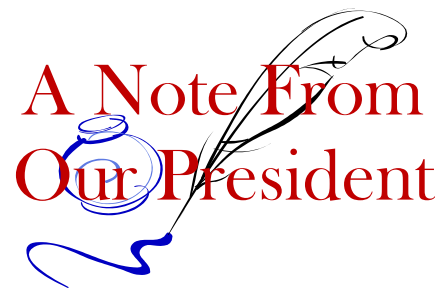
Read the rest here:

<https://justthenews.com/nation/technology/google-confirms-it-notifies-children-if-their-parents-are-monitoring-their>

(Continued from page 1)

speakers; many of whom performed multiple presentations

- Establishing a signed agreement with a new conference production company: Secret Sauce Events, LLC
- Establishing an agreement with Cleared Careers, LLC to sponsor and facilitate two annual ISSA-COS job fairs
- Hosting a virtual version of the annual Peak Cyber CTF; sponsored and facilitated by Splunk and Epoch Concepts
- Hosting the first ever virtual 2-day Peak Cyber Conference; a subset of the Peak Cyber Symposium and this year including 650+ attendees from across the globe
- Establishing Strategic Partnerships with the National Cyber Exchange (NCX), Discover Goodwill, and the Info-Tech Research Group resulting in added membership benefits for our members
- Hosting 23 ISSA-COS Online Presentation Sessions in lieu of in-person, monthly chapter meetings
- The addition of 72 new members and 155 renewing members for ISSA-COS
- The awarding of over 2,000 CPE/CEU credits to members of ISSA-COS
- Representation on four different Social Media platforms: FaceBook, Twitter, LinkedIn, and Instagram
- Collaboration with and mutual support for events with 30 different community partners
- Awarding of the first ever ISSA-COS "Summit" Award to Ms. Colleen Murphy, ISSA-COS Past President for her outstanding volunteer services resulting in the elevation of others within the COS Cybersecurity community and/or industry.



To sum it all up, 2020 was an excellent year for our chapter. We are grateful to all our members, general volunteers, and staff volunteers for contributing their time, talents, and efforts. Now, let us look ahead at 2021 to see what exciting opportunities await all of us!

In 2021, ISSA-COS will maintain our virtual platform for the first quarter (January, February, and March). We hope to resume in-person events in the second quarter starting April but, only time will tell if this will be possible. Regardless of when we resume in-person events, ISSA-COS will return to our traditional schedule of core events (i.e., monthly chapter meetings and Saturday mini seminars) in January. In the previous years, we hosted both a dinner and lunch meeting each month. In 2021, we will utilize our newly implemented virtual platform to record and possibly live-stream our dinner meetings. These new viewing options will enable us to cancel our lunch meetings and thereby, eliminate the cost and manpower required to host our lunch meetings. Plus, the recorded dinner meetings will enable us to offer on-demand playback capability so members can view the event at their convenience – and still earn full CPE/CEU credits!

Our Saturday mini seminars will also be recorded for future playback. Due to the extended nature of our mini seminars, we have not yet determined if live-streaming will be a viable option. We are still researching this option will let our members know if it becomes possible. In 2021, our plan for mini seminars is to turn up the heat and provide more robust hands-on training experiences than in the past. Since the content of our mini seminars fall under our training program, many of our mini seminars may spur Ad Hoc training events throughout the year. This will enable ISSA-COS to provide continual training experiences that can be tailored in complexity to the participants on any given day. This represents a significant improvement and value-added benefit for our members!

In 2021 we will resume our focused on Special Interest Groups (SIGs) by hosting what will become an annual half-day Cyber SIG Summit each June. This event will include presentations specific to each of the eight SIGs recognized by our chapter. Following the final presentations, ISSA-COS will host a community wide Cyber Social event designed to allow networking time for the professionals who attended the summit with others who did not.

Of course, 2021 will continue to include our two annual symposiums: The Cyber Focus Symposium held each Spring, and The Peak Cyber Symposium held each Fall. Based on agreements solidified in 2020, the composition of our symposiums have taken on a more defined, predictable schedule of events. As such, each symposium will include an ISSA-COS Job Fair, ISSA-COS Capture-the-Flag Challenge, and a Theme-based one- or two-day conference. We also hope to incorporate our Girl Scout Cyber Camps into these events but, admittedly, more planning needs to take place before we can confidently announce this feature. Still, the addition of a formal job fair is the fulfillment of a long-sought benefit to our members and one we are finally happy to make available.

Finally, in 2021, we will solidify the year with the inaugural ISSA-COS STAR Awards. This event will replace previous Annual Chapter Celebrations and Annual Award Ceremonies also held in the December timeframe. Our vision for this event is to offer recognition of our chapter members through formal acknowledgements. We will also announce explicit awards bestowed upon specific individuals within various meaningful categories.

(Continued on page 5)



(Continued from page 4)

As you can see, our chapter is prepared to kick-off the new year in fine fashion with lots of exciting events to look forward too. We have a full roster of board members and key personnel ready to get to work and a strong community backing us up. I hope all our member find value in the events we have in store and will encourage and contribute to our success. Please remember we always well first time (and second time) guest to our events and hope everyone will invite someone. Our members are our greatest asset so, let us all try to strengthen our chapter through continued growth. In closing, I thank everyone for a wonderful 2020 and say, "Welcome to 2021!"

Sincerely,

Ernest

CISA Releases CISA Insights and Creates Webpage on Ongoing APT Cyber Activity

Original release date: December 23, 2020

CISA is tracking a known compromise involving SolarWinds Orion products that are currently being exploited by a malicious actor. An advanced persistent threat (APT) actor is responsible for compromising the SolarWinds Orion software supply chain, as well as widespread abuse of commonly used authentication mechanisms. If left unchecked, this threat actor has the resources, patience, and expertise to resist eviction from compromised networks and continue to hold affected organizations at risk.

In response to this threat, CISA has issued CISA Insights: [What Every Leader Needs to Know About the Ongoing APT Cyber Activity](#). This CISA Insights provides information to leaders on the known risk to organizations and actions that they can take to prioritize measures to identify and address these threats.

CISA has also created a new [Supply Chain Compromise webpage](#) to consolidate the many resources—including [Emergency Directive \(ED\) 21-01](#) and Activity Alert [AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations](#)—that we have released on this compromise. CISA will update the webpage to include partner resources that are of value to the cyber community.

To read the latest CISA Insights, visit [CISA.gov/insights](https://cisa.gov/insights). For more information on the SolarWinds Orion software compromise, visit [CISA.gov/supply-chain-compromise](https://cisa.gov/supply-chain-compromise).

2020
A Year To Remember!

2020 Monthly Guest Speakers

Mr. Ernest Campos	Mr. Trent Brunnell Sr.	Ms. Nina Di Francisco	Mr. Thomas Russell
Mr. William "Bill" Vivian	Mr. Peter Sopczak	Ms. Christine Coz	Ms. Jennifer Kurtz
Mr. Justin Whitehead	Mr. Sean Deuby	Mr. Frank Gearhart	Mr. James Lacey
Mr. Art Cooper	Mr. Clark Brown	Mr. Nick Tait	Ms. Colleen Murphy
Mr. Wally Magda	Ms. Erin Plemons	Mr. Michael Wylie	Ms. Erin Beffa
Dr. Erik Huffman	Ms. Lori Hayes	Mr. Derick Lopez	Ms. Erin Miller
Mr. Jay Carson	Mr. Peter Archibald	Mr. Vincent Persichetti	
Mr. Rob Carson	Mr. Jeff Hsiao	Mr. Sean Callahan	
Mr. Mark Spencer	Mr. Michael Lee	Rear Admiral (ret.) Hank Bond	
Mr. Ryan Dozier	Mr. Jeffrey Armstrong	Mr. Terry Bradley	
Ms. Jothi Dugar	Mr. Jeff Tomkiewicz	Ms. Vanessa Johnson	

2020 CYBER FOCUS SYMPOSIUM

Venue Sponsor	UCCS
Production Company	Secret Sauce Events, LLC
Guest Speaker	Dr. Jim Crowder
Guest Speaker	Kelly Misata
Guest Speaker	Nathan Touns
Guest Speaker	Greg Williams
Guest Speaker	Rodney Gullatte Jr.
Guest Speaker	Darla Lindt
Guest Speaker	Steve Winterfield
Guest Speaker	Todd Cronin
Guest Speaker	Jordan "Cancer" Scott
Guest Speaker	Greg Roman
Guest Speaker	Sam Ceccola
Sponsors/Exhibitors	As Listed





2020 PEAK CYBER SYMPOSIUM

Production Company	Secret Sauce Events, LLC
Production Company	Global Events Management, LLC
Virtual Platform Company	Whova!
PCS Job Fair Sponsors/Facilitators	Cleared Careers, LLC
PCS CTF Sponsors/Facilitators	Splunk> and Epoch Concepts
Emcee	Halie Anthony
Emcee	Frank Gearhart
Guest Speakers	Visit: www.peakcyberco.com
Sponsors/Exhibitors	Visit: www.peakcyberco.com
Virtual Booth Volunteer	Mike Crandall
Virtual Booth Volunteer	Jeff Tomkiewicz
Virtual Booth Volunteer	Katie Martin
Virtual Booth Volunteer	Pat Sheehan
Virtual Booth Volunteer	Jay Carson

JMark Services *nc.*

splunk>



Hewlett Packard
Enterprise



WWW.PEAKCYBERCO.COM



2020 NEW MEMBERS

Anthony Carter	Kirsten Mullican	Christopher J McCarty	Drew Koch	John Geiger	Rodney Gullatte Jr.
Brian Pumilia	Lynn Burns	Majestic Dwyer	Seth Foley	Dan Lee	Julia Johnson
Jasmine C. Nichols	David J. Berkowitz	Chad Eckles	Michael Fragola	Christopher Scheirer	Kelli Blanchard
Curtis Brown	Jennifer Carlson	Ebony Bolt	Carl Landers	James Madden	Michael McFadden
Matthew Smith	Christopher J. Tarrant	Derek J. Steel	Timothy Chessmore	Alexander Johnson	Cameron Landreth
Halie Anthony	Deidre LaCour	Sandra Lewis	Tracy Vandeventer	Lindsey Chernoff	Rachel Green
Vincent Persichetti	James Barrett	Jeff Hendron	Jeri M. La May	Joseph Rogers	Michael Quinlan
Jo Beckwith	Cecil Wilkinson	William Vint	Lewis Johnson	Kyle Damon	Eric Crump
Craig Bradley Caviness	Dr. Ronald Davis	Lisa Hernandez	Peter Rivera	Patricia Marie March	Scott Walker
Elisa Patterson	Daniel Pocius	Michael Hooper	Tani Evans	Sean Patrick Callahan	Casey McClure
Samuel C Mercer	Eric Thompson	Ashley N. Gilbert	Tony Gooch	Michael McCarty	Nick Williams
Atta Owusu Sarpong	Robert William Benjamin	Larry O'Brien	Deon Ware	Justin Holmstrom	Heather Lawrence



ISSA-COS

2021 Schedule of Events

Monthly Events

Chapter Meetings (6:00 – 7:30 PM) ¹

Tuesday, January 19, 2021 ²

Tuesday, February 16, 2021 ²

March – Quarterly/Annual Events

Tuesday, April 20, 2021 ³

Tuesday, May 18, 2021 ³

June – Quarterly/Annual Events

Tuesday, July 20, 2021 ³

Tuesday, August 17, 2021 ³

September – Quarterly/Annual Events

Tuesday, October 19, 2021 ³

Tuesday, November 16, 2021 ³

December – Quarterly/Annual Events

¹ Light Dinner Provided @ 5:30 PM

² Virtual Meeting; Recorded Playback Available

³ In-person Meeting; Recorded Playback Available

Mini – Seminars (9:00 – 12:00 PM) ¹

Saturday, January 23, 2021 ²

Saturday, February 20, 2021 ²

March – Quarterly/Annual Events

Saturday, April 24, 2021 ³

Saturday, May 22, 2021 ³

June – Quarterly/Annual Events

Saturday, July 24, 2021 ³

Saturday, August 21, 2021 ³

September – Quarterly/Annual Events

Saturday, October 23, 2021 ³

Saturday, November 13, 2021 ³

December – Quarterly/Annual Events

¹ Continental Breakfast Provided @ 8:30 AM

² Virtual Meeting; Recorded Playback Available

³ In-person Meeting; Recorded Playback Available

Quarterly Events

Virtual Security + CE Reviews

Saturday, March 6, 2021

Saturday, March 13, 2021

Saturday, March 20, 2021

Saturday, September 11, 2021

Saturday, September 18, 2021

Saturday, September 25, 2021

Cyber Focus Symposium (CFS)

April 2021

CFS Girl Scout Cyber Camp

April 20-22, 2021

CFS Job Fair

CFS Capture-the-Flag Challenge

CFS Conference

Virtual CISSP Review

Saturday, June 5, 2021

Friday, June 11, 2021

Saturday, June 12, 2021

Saturday, June 19, 2021

Friday, June 25, 2021

Saturday, June 26, 2021

Peak Cyber Symposium (PCS)

September 2021

PCS Girl Scout Cyber Camp

September 14 – 16, 2021

PCS Job Fair

PCS Capture-the-Flag Challenge

PCS Conference



Annual Events

² Annual President's Address	>>	Tuesday, January 5, 2021 (6:00 – 7:00 PM)
³ Annual Cyber SIG Summit	>>	Friday, June 18, 2021 (1:00 – 5:00 PM)
⁴ Annual Cyber Social	>>	Friday, June 18, 2021 (5:00 – 9:00 PM)
Annual Chapter Elections	>>	Oct – Nov 2021 (Details TBA)
⁴ Annual STAR Awards	>>	Friday, December 3, 2021 (5:00 – 9:00 PM)

² Virtual Meeting; Recorded Playback Available | ³ In-person Meeting; Recorded Playback Available | ⁴ In-person Meeting Only

For additional information, contact info@issa-cos.org or visit www.issa-cos.org.



2020 ISSA INTERNATIONAL RECOGNITIONS

Senior Member	Amy Coffman
Senior Member	Derick Lopez
Senior Member	James Asimah
Fellow	Kurt Danis
Distinguished Fellow	Scott Frisch
Distinguished Fellow	Warren Pierce
Volunteer of the Year	Jay Carson
Honor Roll	Scott Frisch

Defense officials look at splitting up NSA, CYBERCOM

By Caitlyn McFall, FoxNews, December 19, 2020

Top Defense officials are considering breaking the National Security Agency (NSA) away from the Cyber Command (CYBERCOM), a move that the chairman of the House Armed Services Committee said made him "profoundly concerned."

Rep. Adam Smith, D-Wash., sent a letter to acting Department of Defense Secretary Christopher Miller, objecting to the department's attempts to separate the security commands "without consulting Congress or meeting the conditions required by law."

The NSA and CYBERCOM work closely together under the Department of Defense, and are both overseen by four star Gen. Paul M. Nakasone.

The push to separate them during President Trump's final days in office, is the latest move by the Trump administration to shake up the Pentagon.

Miller was named acting secretary in early November, after Trump unexpectedly sacked Defense Secretary Mark Esper.

Read the rest here:

<https://www.foxnews.com/us/defense-officials-splitting-up-nsa-cyber-command>

2020 Operations

ANNUAL AUDIT COMMITTEE

Committee Chair	Chris Edmondson
-----------------	-----------------

IT COMMITTEE

Committee Chair	Pat Sheehan
-----------------	-------------

Committee Member	April Frost
------------------	-------------

Committee Member	Wayne Lo
------------------	----------

SPEAKERS BUREAU COMMITTEE

Committee Chair	Jay Carson
-----------------	------------

Committee Member	Marcelle Licciardi
------------------	--------------------

MENTORING COMMITTEE

Committee Chair	Carissa Nichols
-----------------	-----------------

TRAINING COMMITTEE

Committee Chair	Mark Heinrich
-----------------	---------------

Committee Member – Instructors	Multiple
--------------------------------	----------

Committee Member – Facilitators	Multiple
---------------------------------	----------

Committee Member – Curriculum	Multiple
-------------------------------	----------

Authors	
---------	--

MEDIA/NEWSLETTER COMMITTEE

Newsletter Committee Chair	Don Creamer
----------------------------	-------------

Photographer	Warren Pierce
--------------	---------------

Graphic Artist	Aaron Johnson
----------------	---------------





Girl Scouts Cyber Badge Camp

Girl Scouts Program Coordinator	Anna Parrish
PPCC Intern – Curriculum Author	Zavier Morales
PPCC Intern – Curriculum Author	Paul Baumgarten
PPCC Intern – Curriculum Author	Matt Huyge

ANNUAL ELECTION COMMITTEE

Committee Chair	Colleen Murphy
Committee Member	Frank Gearhart
Committee Member	Mark Spencer
Committee Member	Pat Laverty



ISSA-COS SALUTES ALL OUR CURRENT
COMMUNITY PARTNERS!

THANK YOU FOR ALL YOU DO TO SUPPORT OUR
CHAPTER AND OUR COMMUNITY!











**TOGETHER WE
ARE STRONGER**

WWW.ISSA-COS.ORG

Strategic Partners



Current Annual Chapter Sponsors

Platinum	Gold	Silver	Bronze	Single Event	Material/Venue
			 	 	    

Become a 12-month Sponsor Today!



2020 KEY PERSONNEL

Deputy Vice President of Training	Phebe Swope
Deputy Director of Certifications	Luke Walcher
Deputy Director of Communications	Ryan Evan
Speakers Bureau Committee Chair	Jay Carson
IT Committee Chair	Pat Sheehan
Mentoring Committee Chair	Carissa Nichols
Newsletter Committee Chair	Don Creamer
Training Committee Chair	Mark Heinrich
Program Coordinator	Anna Parrish
Past President	Colleen Murphy
Past President	Frank Gearhart
Past President	Pat Lavery
Past President Emeritus	Mark Spencer

2020 BOARD MEMBERS

President & Chairman of the Board	Ernest Campos
Vice President	Mike Crandall
Executive Vice President	Scott Frisch
Recorder/Historian	Andrea Heinz
Treasurer	Dennis Schorn
Vice President of Membership	Steven Mulig
Vice President of Training	Mark Heinrich
Director of Communications	Christine Mack
Director of Certifications	Derick Lopez
Director of Professional Outreach	Katie Martin
Member-at-Large #1	Art Cooper
Member-at-Large #2	Jim Blake
Member-at-Large #3	James Asimah
Member-at-Large #4	Dennis Kater

Special Recognition!



Awarded for outstanding
volunteer services
resulting in the elevation
of others within the COS
Cybersecurity community
and/or industry.

Colleen Murphy
ISSA-COS SUMMIT AWARD



Congratulations

to our members, our chapter, and to
our community for a wonderful year!





Stepping Up! with ISSA-COS

OPEN LEADERSHIP POSITIONS

- Deputy Treasurer
- Deputy Recorder/Historian
- Deputy Vice President of Training
- Deputy Vice President of Membership
- Deputy Director of Professional Outreach
- Deputy Director of Communications
- Speakers Bureau Committee Chairperson
- Mentoring Committee Chairperson



**An excellent way to help
advance your career!**

For more information or to
volunteer, contact:

info@issa-cos.org



1/5/2021

ISSA-COS Annual President's Address

Speaker: Mr. Ernest Campos, *President, ISSA-COS*

1/19/2021

ISSA-COS Chapter Meeting

Speaker: TBD

1/23/2021

ISSA-COS Mini-Seminar

Speaker: TBD

Instructions & Credit for Online Playbacks of ISSA-COS Training Sessions

- Video playbacks are available to ISSA-COS members within 3-days
- Navigate to the www.issa-cos.org website
- Login using your COS Chapter credentials
- Navigate to "Training" and select the desired month
- Select the desired presentation and enjoy the playback
- Upon completion of the playback, email: certification@issa-cos.org and identify the month and session number for the episode you viewed

Academics turn RAM into Wi-Fi cards to steal data from air-gapped systems

By Catalin Cimpanu, ZD Net, December 15, 2020

Trend Micro's security researchers have identified a new macOS backdoor that they believe is used by the Vietnamese threat actor OceanLotus.

Academics from an Israeli university have published new research today detailing a technique to convert a RAM card into an impromptu wireless emitter and transmit sensitive data from inside a non-networked air-gapped computer that has no Wi-Fi card.

Named **AIR-FI**, the technique is the work of Mordechai Guri, the head of R&D at the Ben-Gurion University of the Negev, in Israel.

Over the last half-decade, Guri has led tens of research projects that investigated stealing data through unconventional methods from air-gapped systems.

These types of techniques are what security researchers call "*covert data exfiltration channels*." They are not techniques to break into computers, but techniques that can be used to steal data in ways defenders aren't expecting.

Such data exfiltration channels are not a danger for normal users, but they are a constant threat for the administrators of air-gapped networks.

Air-gapped systems are computers isolated on local networks with no external internet access. Air-gapped systems are often used on government, military, or corporate networks to store sensitive data, such as classified files or intellectual property.

While AIR-FI would be considered a "stunt hack" in the threat model of normal users, it is, however, the type of attack that forces many companies to reconsider the architecture of their air-gapped systems that store high-value assets.

How Air-Fi Works

Read the rest here:

<https://www.zdnet.com/article/academics-turn-ram-into-wifi-cards-to-steal-data-from-air-gapped-systems/>



Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data

Original release date: December 10, 2020

Summary

This Joint Cybersecurity Advisory was coauthored by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC).

The FBI, CISA, and MS-ISAC assess malicious cyber actors are targeting kindergarten through twelfth grade (K-12) educational institutions, leading to ransomware attacks, the theft of data, and the disruption of distance learning services. Cyber actors likely view schools as targets of opportunity, and these types of attacks are expected to continue through the 2020/2021 academic year. These issues will be particularly challenging for K-12 schools that face resource limitations; therefore, educational leadership, information technology personnel, and security personnel will need to balance this risk when determining their cybersecurity investments.



Technical Details

As of December 2020, the FBI, CISA, and MS-ISAC continue to receive reports from K-12 educational institutions about the disruption of distance learning efforts by cyber actors.

Ransomware

The FBI, CISA, and MS-ISAC have received numerous reports of ransomware attacks against K-12 educational institutions. In these attacks, malicious cyber actors target school computer systems, slowing access, and—in some instances—rendering the systems inaccessible for basic functions, including distance learning. Adopting tactics previously leveraged against business and industry, ransomware actors have also stolen—and threatened to leak—confidential student data to the public unless institutions pay a ransom.

According to MS-ISAC data, the percentage of reported ransomware incidents against K-12 schools increased at the beginning of the 2020 school year. In August and September, 57% of ransomware incidents reported to the MS-ISAC involved K-12 schools, compared to 28% of all reported ransomware incidents from January through July.

The five most common ransomware variants identified in incidents targeting K-12 schools between January and September 2020—based on open source information as well as victim and third-party incident reports made to MS-ISAC—are Ryuk, Maze, Nefilim, AKO, and Sodinokibi/REvil.

Malware

Figure 1 identifies the top 10 malware strains that have affected state, local, tribal, and territorial (SLTT) educational institutions over the past year (up to and including September 2020). Note: These malware variants are purely opportunistic as they not only affect educational institutions but other organizations as well.

Zeus and Shlayer are among the most prevalent malware affecting K-12 schools.

- Zeus is a Trojan with several variants that targets Microsoft Windows operating systems. Cyber actors use Zeus to infect target machines and send stolen information to command-and-control servers.
- Shlayer is a Trojan downloader and dropper for MacOS malware. It is primarily distributed through malicious websites, hijacked domains, and malicious advertising posing as a fake Adobe Flash updater. **Note:** Shlayer is the only malware of the top 10 that targets MacOS; the other 9 affect Microsoft Windows operating systems

Distributed Denial-of-Service Attacks

Cyber actors are causing disruptions to K-12 educational institutions—including third-party services supporting distance learning—with distributed denial-of-service (DDoS) attacks, which temporarily limit or prevent users from conducting daily operations. The availability of DDoS-for-hire services provides opportunities for any motivated malicious cyber actor to conduct disruptive attacks regardless of experience level. **Note:** DDoS attacks overwhelm servers with a high level of internet traffic originating from many different sources, making it impossible to mitigate at a single source.

[Click here](#) for a PDF version of this report.

The Worst Hacks of 2020, a Surreal Pandemic Year

By Lily Hay Newman, *Wired*, December 27, 2020

What a way to kick off a new decade. 2020 showcased all of the digital risks and cybersecurity woes you've come to expect in the modern era, but this year was unique in the ways Covid-19 radically and tragically transformed life around the world. The pandemic also created unprecedented conditions in cyberspace, reshaping networks by pushing people to work from home en masse, creating a scramble to access vaccine research by any means, generating new fodder for criminals to launch extortion attempts and scams, and producing novel opportunities for nation-state espionage.

Here's WIRED's look back at this strange year and the breaches, data exposures, ransomware attacks, state-sponsored campaigns, and digital madness that shaped it. Stay safe out there in 2021.

SolarWinds Supply Chain Hack

On Tuesday, December 8, the well-respected cybersecurity and incident response firm FireEye made a stunning disclosure. The company had suffered a breach, and hackers had stolen some of the firm's internal threat-intelligence data as well as a cache of its "red team" hacking tools—used to probe the systems of paying customers for weaknesses so they can be fixed before attackers find them. In itself, the FireEye breach, which *The Washington Post* quickly attributed to Russian state-backed hackers, was significant but not a catastrophe. What no one knew that day, though, was that 18,000 other shoes were about to drop.

Beginning on Sunday, December 13, news broke in waves that United States government agencies like the Commerce, Treasury, Homeland Security, and Energy Departments, corporations, and international targets had all been victims of a massive nation-state espionage campaign. The hackers, who have widely been reported as Russian, were on a rampage that was largely made possible by what's known as a supply chain attack. In other words, all of the attacks were made possible by one initial compromise, in this case at the IT infrastructure firm SolarWinds. Hackers had breached the company as early as October 2019 and planted malicious code in software updates for its network-monitoring tool, Orion. Without knowing it, any customer that installed an Orion patch released between March and June was also planting a Russian backdoor on their own network.

There is also some evidence that the attackers compromised victims through other means aside from the SolarWinds breach, but through that one intrusion the attackers created access for themselves in roughly 18,000 SolarWinds customer networks, according to the company. The impact of the attack varied among victims. In some cases the hackers planted a backdoor but didn't go any farther. In other cases they used the access just long enough to figure out that they didn't care about the target. And for an unlucky subset, the attackers moved deep within victim networks for reconnaissance and data exfiltration. For example, critical infrastructure companies like more than a dozen in the oil, electric, and manufacturing sectors seem to have installed the backdoor, but it's not clear how extensively they were actually infiltrated by attackers. The situation underscores the threat posed by supply chain attacks, because they can efficiently undermine all of a company's customers in one fell swoop.

Russian hackers have used the technique before, sometimes with more expressly destructive goals. The SolarWinds attacks so far seem to have been largely for espionage, though some experts warn that it's too soon to tell whether there was a destructive component. Even if the attacks were purely for information-gathering, which is usually a globally accepted activity, some politicians and researchers say that the intrusions cross a line or are out of step with espionage norms because of their scale and scope. As former CIA agent Paul Kolbe put it last week in a *New York Times* essay, though, "The United States is, of course, engaged in the same type of operations at an even grander scale. We are active participants in an ambient cyberconflict that rages, largely unseen and unacknowledged, across the digital globe. This is a struggle that we can't avoid, and there is no need to play the victim." The question now is how the United States will respond to the SolarWinds hacking spree and approach digital espionage and conflict in the future as the Trump administration ends and the Biden administration begins.

Twitter

In July, a wave of stunning takeovers swept across Twitter, hijacking the accounts of Joe Biden, Barack Obama, Elon Musk, Kanye West, Bill Gates, and Michael Bloomberg, as well as major corporate accounts like that of Apple and Uber. The accounts tweeted out variations of a common theme: "I am giving back to the community. All Bitcoin sent to the address below will be sent back doubled! If you send \$1,000, I will send back \$2,000. Only doing this for 30 minutes."

Read the rest here:

<https://www.wired.com/story/worst-hacks-2020-surreal-pandemic-year/>





NIST CYBERSECURITY and PRIVACY PROGRAM

NIST Releases Supplemental Materials for SP 800-53: Analysis of Changes Between Revisions 4 and 5, and Control Mappings

New supplemental materials for NIST Special Publication (SP) 800-53 Revision 5, ***Security and Privacy Controls for Information Systems and Organizations***, are available for download to support the December 10, 2020 errata release of SP 800-53¹ and SP 800-53B², ***Control Baselines for Information Systems and Organizations***. Errata updates to SP 800-53 Rev. 5 and SP 800-53B address errors, omissions, and clarifications based on internal review and stakeholder feedback—they do not fundamentally change the underlying technical specifications. Each document includes an errata table that identifies the updates.

New resources are intended to support organizations transitioning from SP 800-53 Revision 4 to Revision 5; they are posted in the Supplemental Material section of the SP 800-53 publication details¹. These include an analysis of the changes from Revision 4 to Revision 5 of SP 800-53 and a mapping of the Appendix J Privacy Controls (Revision 4) to Revision 5. Control mappings to the NIST Cybersecurity Framework, Privacy Framework, and ISO 27001 are also provided.

Specifically, the supplemental materials include:

A comparison of the NIST SP 800-53 Revision 5 controls and control enhancements to Revision 4

The spreadsheet describes the changes to each control and control enhancement, provides a brief summary of the changes, and includes an assessment of the significance of the changes. *Note that this comparison was authored by The MITRE Corporation for the Director of National Intelligence (DNI) and is being shared with permission by DNI.*

Mapping of the Appendix J Privacy Controls (Revision 4) to Revision 5

The spreadsheet supports organizations using the privacy controls in Appendix J of SP 800-53 Revision 4 that are transitioning to the integrated control catalog in Revision 5.

Mappings between NIST SP 800-53 and other frameworks and standards

The mappings provide organizations a general indication of SP 800-53 control coverage with respect to other frameworks and standards. When leveraging the mappings, it is important to consider the intended scope of each publication and how each publication is used; organizations should not assume equivalency based solely on the mapping tables because mappings are not always one-to-one and there is a degree of subjectivity in the mapping analysis.

The Open Security Control Assessment Language (OSCAL) version³ of the SP 800-53 Revision 5 controls and SP 800-53B control baselines and spreadsheet versions of controls/baselines will be available soon.

For questions, comments, and feedback, please contact sec-cert@nist.gov.

Publication details:

1. SP 800-53 Revision 5, <https://no-click.mil/?https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

2. SP 800-53B, <https://no-click.mil/?https://csrc.nist.gov/publications/detail/sp/800-53b/final>

OSCAL version of 800-53 controls:

3. <https://no-click.mil/?https://github.com/usnistgov/oscal-content/tree/master/nist.gov/SP800-53>

MENTORING PROGRAM

The ISSA-COS Mentoring Program provides a connection between individuals (mentees) seeking career guidance, industry information, or personal encouragement with individuals (mentors) who have an aptitude for sharing their career experiences, industry resources, and personal talents for the benefit of the mentee. Mentees derive from every conceivable background and exist at every stage of professional development. Mentoring sessions are designed to ensure the confidentiality, integrity, and availability of information shared between the participants.

To help facilitate the mentoring process, ISSA-COS has adopted the S.M.A.R.T. goal setting model to safeguard a consistent development process that is equally understood and honored by mentees and mentors alike. As such, the Mentoring Program supports the following objectives of ISSA-COS:

- Promote increased professional education opportunities for members
- Provide career guidance and professional development approaches
- Encourage balance between technical skillsets and soft skills such as time management, task management, workplace conduct, and business savvy
- Increase member knowledge of available resources designed to strengthen skillsets
- Encouraging an open exchange of Cybersecurity related techniques, approaches, and problem-solving skills
- Promote member education and awareness of Cybersecurity security issues and recommended strategies to combat the issues
- Providing opportunities for mentees and mentors to network with other professionals and share their lessons learned from their individual mentoring experiences.

**For more information
about mentoring,
email:
[mentorship
@issa-cos.org](mailto:mentorship@issa-cos.org)**



Cyber Spotlight – PARTY!!

ISSA-COS is turning **30** in 2021!

Initiative to document ISSA-COS Chapter History

Interviews with past/current **Presidents**

Interviews with past/current **Board Members**

Interviews with past/current **General Members**

Interviews with **Community Partners**





WWW.ISSA-COS.ORG

Chapter Officers:

President*: Ernest Campos

Vice President*: Michael Crandall

Executive Vice President*: Scott Frisch

Treasurer: Dennis Schorn

- Deputy: **Vacant**

Recorder/Historian: Andrea Heinz

- Deputy: **Vacant**

Dir. of Professional Outreach: Katie Martin

- Deputy: **Vacant**

Director of Communications : Christine Mack

- Deputy: Ryan Evan

Director of Certifications: Derick Lopez

- Deputy: Luke Walcher

Vice President of Membership: Steven Mulig

- Deputy: **Vacant**

Vice President of Training: Jeff Tomkiewicz

- Deputy: Phebe Swope

Member at Large 1: Art Cooper

Member at Large 2: Jim Blake

Member at Large 3: James Asimah

Member at Large 4: Jay Carson

Committee Chairs:

Annual Audit: Chris Edmondson

Training: Mark Heinrich

Mentorship Committee Chair: Carissa Nichols

Media/Newsletter: Don Creamer

IT Committee: Patrick Sheehan

Speaker's Bureau: William (Jay) Carson

Girl Scouts Cyber Badge Camp: Anna Parrish

Annual Election: Colleen Murphy

* Executive Board Members

The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Article for the Newsletter?

We are always looking for articles that may be of interest to the broader Colorado Springs cyber community.

Send your article ideas to the Newsletter at:

newsletter@issa-cos.org

Past Senior Leadership

President Emeritus: Dr. George J. Proeller

President Emeritus: Mark Spencer

Past President: Mike O'Neill

Past President: Pat Laverty

Past President: Cindy Thornburg

Past President: Frank Gearhart

Past President: Colleen Murphy

Divers recover a WWII Enigma Machine from the Baltic Sea

By Kiona N. Smith, ArsTechnica, December 27, 2020



When Nazi naval officers tossed their ship's Enigma encryption machine overboard, they probably thought they were putting the device beyond anyone's reach. Blissfully unaware that Allied cryptanalysts in Poland and at Bletchley Park in the UK had broken the Enigma code, the Nazis had standing orders to destroy their encryption devices to keep them out of Allied hands. Eighty years later, divers found the once-secret device tangled in an abandoned fishing net on the seafloor, and now it's set to be put on display for everyone to see. LOL, Nazis pwned.

Research diver Florian Huber and his colleagues were trying to clear abandoned fishing nets from the Bay of Gelting, on the Baltic Sea near the German-Danish border, when they found the artifact. Derelict nets and other discarded fishing gear can still entangle fish, sea turtles, diving birds, and marine mammals like seals and dolphins. The World Wildlife Fund had hired the divers to clear them in November 2020.

Read the rest here:

<https://arstechnica.com/science/2020/12/divers-recover-a-wwii-code-machine-from-the-baltic-sea/>