CELEBRATING

2001–2021 Anniversary Report

CIAS

About the CIAS

The Center for Infrastructure Assurance and Security (CIAS) was established at The University of Texas at San Antonio (UTSA) in June of 2001 as part of UTSA's creation of a cybersecurity program. The university was recognized in 2002 by the National Security Agency as a leader in the field of infrastructure assurance and security and was designated a Center of Academic Excellence in Information Assurance Education.

Our Vision

The leader in advancement of state, local, tribes and territories (SLTT) cybersecurity capabilities and collaboration.

Our Mission

Deliver quality research, training, competitions, exercises and educational game programs to advance community and organizational cyber security capabilities and collaboration.

cias.utsa.edu

cias@utsa.edu

210.458.2119

/cias.utsa

/ciascybersec

CONTENTS

LETTER FROM THE DIRECTOR

Twenty years sounds like a long time, and for university centers it is. But, at the same time, those 20 years have gone by incredibly fast for the CIAS.

I started as the technical director for the UTSA Center for Infrastructure Assurance and Security. Dr. Glenn Dietrich, the first director for the CIAS, hired me to help start a cybersecurity program at UTSA. Since that time, we have accomplished a lot and have seen the cybersecurity program at UTSA grow into one that has garnered a national reputation and has helped thousands of individuals prepare for careers in cybersecurity.

Since 2001, the CIAS has received more than $71.8 million in grants, contracts and donations making it one of the most successful centers at UTSA. We have seen the cybersecurity program at UTSA receive national attention: a 2014 Ponemon Institute study ranked UTSA No. 1 in the nation at the undergraduate level followed in 2016 with a No. 2 graduate program ranking by universities.com. The National Security Agency has awarded UTSA all three of its national Centers of Academic Excellence designations – in Cyber Defense, Research and Cyber Operations – placing UTSA in a very select category of universities. The CIAS, along with the Institute for Cyber Security and the Center for Cybersecurity and Analytics, has played a significant role in the current reputation of UTSA.

In addition to providing the initial research funding to jumpstart cybersecurity research at UTSA, the CIAS conducted the first community cybersecurity exercise, called Dark Screen, in San Antonio, Texas, then followed it with several other cybersecurity exercises at the state and community levels. We have created the best-known collegiate cybersecurity defensive competition, the National Collegiate Cyber Defense Competition (NCCDC) and followed that competition by being one of the co-founders of CyberPatriot, a cyber competition for middle and high school students. We continue to be the technology component running the CyberPatriot program, which is run by the Air Force

Association (AFA), and is now the single largest cybersecurity competition in the world introducing tens of thousands of students to cybersecurity.

The CIAS has received several grants from the Department of Homeland Security (DHS) to develop cybersecurity training for state, local, tribal and territorial (SLTT) governments, and we are one of the co-founders for the National Cybersecurity Preparedness Consortium (NCPC). In 2015, we were selected by DHS to become the nation's Information Sharing and Analysis Organization (ISAO) Standards Organization (SO) and we continue to help individuals and organizations from across the nation to establish ISAOs.

We have a strong K-12 cybersecurity program, starting with computer games developed for the Air Force Association's CyberPatriot program that was followed by Cyber Threat Defender: The Collectible Card Game, which is now played in 17 countries. We followed this with additional electronic games as well as two additional card games. We recently announced our Culture of Cybersecurity Campaign partnered with the MITRE Corporation, which features the "CyBear Family"—the cybersecurity equivalent of Smokey and McGruff. These are just some of our accomplishments over the last 20 years —a history we are tremendously proud of.

Looking forward, what do we see in the next 20 years? We will continue with the initiatives in place now, expanding their reach to touch even more individuals. In 2002, we looked at the government's cybersecurity efforts and recognized the weak link were the SLTTs, especially communities. This is where our underlying focus has been and will continue to be. Our programs are aimed at finding and training the individuals today that will make a difference in securing the nation tomorrow. In 2002, we saw the need for a grassroots-level program the nation still needs today. In the last couple of years this has been recognized by DHS as critically important and we are positioned to play a key role in this area in the future. Our research efforts will expand to do even more in creating the technology and processes SLTTs need.

We continue to increase the number of competitions to provide cyber defense-focused events that reach as many individuals as possible. The NCPC is gaining a solid reputation throughout the nation and we will continue to be a major player in that effort, as it is based on a cybersecurity model we developed. Our K-12 and Culture of Cybersecurity initiatives are gaining a strong following and will play a key role in establishing a national Culture of Cybersecurity.

The first 20 years saw us develop a number of initiatives and the next 20 will see us continue to increase our role in improving the nation's cybersecurity posture!

Very Respectfully,

Gregory B. White, Ph.D.
Professor of Computer Science
Director, Center for Infrastructure Assurance and Security
The University of Texas at San Antonio

The Community Cyber Security Maturity Model

The CIAS developed the Community Cyber Security Maturity Model (CCSMM) as a result of lessons learned over several years of working with states and communities to help them develop their own cybersecurity programs. At the time, and at some level still today, most of the nation's cybersecurity focus is at the federal level and the various critical infrastructures. While security for these entities is essential, security at the state and community levels is also important and has not received the same level of attention. Community cybersecurity is arguably the weak link in the nation's cybersecurity chain.

Purpose of the Community Cybersecurity Maturity Model

The Community Cyber Security Maturity Model is a coordinated plan that provides communities, states or local jurisdictions with a framework to identify what is needed to build a cybersecurity program focused on "whole community" preparedness and response to address a cyber incident or attack. Essentially, the CCSMM is a guide that helps communities establish a cybersecurity baseline at the local level. Once established, the baseline can be used to identify cyber-attacks that impact an organization, an entire sector, or cross-sector organizations and agencies in a specific geographic area. It can also be used to communicate with individuals and communities about capabilities and improvement.

The strategies identified in the framework go beyond protecting systems and networks within local government agencies. The CCSMM can assist communities to identify what needs to be done in building a viable and sustainable cybersecurity program, what is needed to prepare to detect a cyber-attack, develop plans to respond during an attack, and determine what to do after an attack has occurred.

The CCSMM incorporates three critical features:

A **yardstick** to measure the current status of a community or state's cybersecurity program and posture

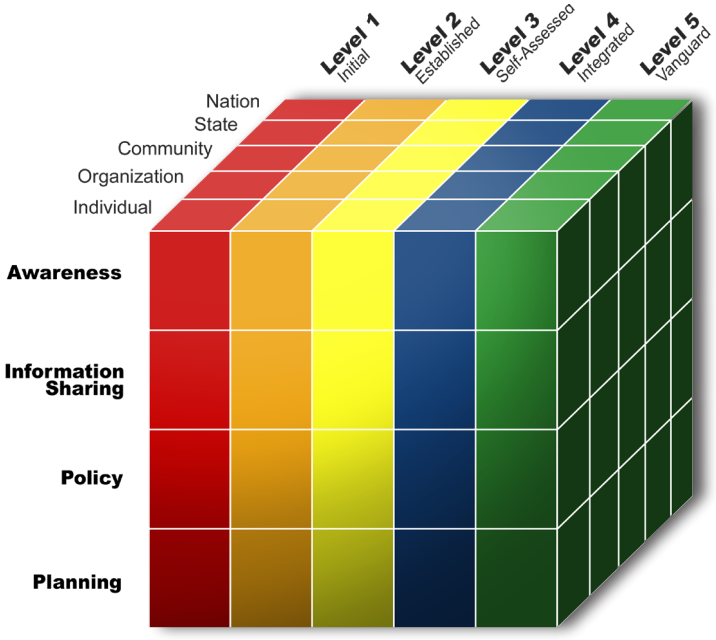
A **roadmap** to help communities and states know what steps are needed to improve their security posture

A **common point of reference** that allows individuals from different communities and states to discuss their individual programs and relate them to each other.

> “COMMUNITY cybersecurity is arguably the weak link in the nation’s cybersecurity chain.”

The 3D Community Cybersecurity Model

The purpose of the 3-D Model is to broaden the capability of the framework allowing it to be flexible and scalable to address all aspects of a cybersecurity program. Expanding the CCSMM into a 3-dimensional model provides the improvement progression for everyone in the nation.



In addition, it can integrate other frameworks such as the National Institute of Standards and Technology’s (NIST) Cyber Security Framework (CSF) (NIST, 2018) and the DoD’s CMMC outlining the security controls necessary for an organization. It can also support the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) (NIST, 2017), which is a resource that categorizes and describes cybersecurity work and the cybersecurity workforce.

The CCSMM can assist communities to identify what needs to be done in building a viable and sustainable cybersecurity program, what is needed to prepare to detect a cyber-attack, develop plans to respond during an attack, and determine what to do after an attack has occurred.

RESEARCH:
Honey Pot Communities

Beginning in 2002, the CIAS conducted a series of community and state cybersecurity exercises around the country. These were successful events in that participants went away having learned about issues related to the importance of cybersecurity within states and communities and how important information sharing is in order to be able to address attacks involving more than one organization.

While participants learned about various cybersecurity issues, a common problem was a lack of understanding concerning where to start implementing a community-wide cybersecurity program. The CIAS studied this issue and determined what was needed was more specific guidance to help states and communities understand where to start and how to progress. The result was the development of the Community Cyber Security Maturity Model (CCSMM), which provided both a way to measure the current maturity of the state's or community's cybersecurity program and guidance to know what steps they could take to improve.

While the CCSMM was a big step forward for states and communities desiring to improve their cybersecurity posture, what was still lacking was more detailed assistance on community cybersecurity attacks and methods to help determine when a community might be experiencing an attack.

Looking Across Multiple Sectors

Information on the right is a summation of the data captured from a Honey Community, called The City of Roadrunner Park. The "city" website that was developed had functions similar to a typical community. 1.2 GB of raw pcap data was gathered.

Number of Sectors	Identified Attacks
*	1,402
1	1,430
2	151
3	52
4	16
5	9

Sector	Identified Attacks
Community	2,319
Water & Sewer	369
Criminal Justice	345
Emergency Response	398
Education	381
Commerce	504

cross-sector collaboration within a community was not only helpful but essential in identifying attacks."

Dr. Keith Harrison, who was then a doctoral student in the Computer Science Department, developed a taxonomy of community attacks and used this in the development of a "honey community"—a fictious community he used to observe attacks on a community to evaluate his taxonomy. What he observed helped him to refine the taxonomy but it also led to an important discovery.

Nearly half of all attacks would have most likely gone unnoticed as a result of the thresholds normally established by organizations to prevent becoming overwhelmed with alerts from their network security devices.

If, however, the community was viewed across all sectors, these attacks were more easily identified leading to the realization that cross-sector collaboration within a community was not only helpful but essential in identifying attacks.

Dr. Harrison's efforts were extended by Dr. Jim Rutherford, another doctoral student at UTSA, who developed deployable sensors to help create a more efficient honey community structure.

Their efforts have resulted in a recent grant from the NSA to continue with this research.

It also illustrates the type of SLTT-focused research that the CIAS is interested in and continues to pursue.

What the Research Showed*

3,060

Number of intrusion detection system (IDS) alerts generated by SNORT

55%

Percentage of attacks that could be seen as an attack on one or more sectors

45%

Percentage of attacks that would NOT have been noticed by any individual sector

On Repeat

Attacks on one sector often reappeared later against another sector

*Data from Harrison, Rutherford, and White. "The Honey Community: Use of Combined Organizational Data for Community Protection." System Sciences (HICSS), 2015 48th Annual Hawaii International Conference, 2015.

RESEARCH
Conducted by the CIAS

When the CIAS was created, it received a total of $5 million from the Department of Defense through a grant sponsored by Senator Kay Bailey Hutchison. A large portion of this grant was intended to be used to help jumpstart the security program at UTSA. The CIAS sent out a call for proposals to faculty members at UTSA for research in cybersecurity. Multiple projects in the College of Business, College of Sciences and College of Engineering were chosen for support by a committee of reviewers from UTSA and the U.S. Air Force.

Research projects included topics like hardware-based intrusion detection, elliptic curve cryptography, detection of steganography and biometric access control methods. This research support was successful in helping professors support graduate students and to initiate a cybersecurity research program at UTSA. After these first two years of research funding, research efforts in the CIAS have focused on issues directly related to the security needs of state, local, tribal and territorial (SLTT) government organizations.

Presentations at the Hawaii International Conference on System Sciences (HICSS)

Over the years, research conducted by the CIAS has led to multiple research papers being presented at the Hawaii International Conference on System Sciences. HICSS has been known worldwide as the longest-standing working scientific conferences in Information Technology Management. Since 1968, HICSS has provided a highly interactive working environment for top scholars from academia and industry from over 60 countries to exchange ideas in areas of information, computer and system sciences.

In 2008, Dr. Greg White and Natalie Sjelin presented their research on the topic of "Cybersecurity and Government Fusion Centers". White and Sjelin argued that there was a need to develop a cyber capability in fusion centers and the importance of government involvement in coordinating a state's, community's or region's cyber defense efforts.

In 2009, White and Sjelin presented their research on "Developing a Community Cyber Security Incident Response Capability". The research addressed the challenges community leaders face in the event of a cyber attack and made various recommendations for what communities can do in preparing for a cyber-attack or incident.

Cutting-edge Training Today

The CIAS has been conducting research for the past 20 years leading to the creation of cutting-edge training that doesn't exist anywhere else.

In 2019, research into the creation of a cyber annex for incident response led to the creation of a FEMA Continuing Training Grant course *AWR-366W – Developing a Cybersecurity Annex for Incident Response*. Research centered on the Community Cyber Security Maturity Model developed by the CIAS led to several FEMA Continuing Training Grant (CTG) courses.

The ISAO SO effort and additional information sharing research has led to the development of the FEMA CTG Course *AWR-381W Establishing an Information Sharing and Analysis Organization*. Additional research with communities and the ISAO SO has also led to the development of FEMA CTG Course *MGT-473 Organizational Cybersecurity Information Sharing*.

More recently in 2020, the CIAS was awarded a grant by the Department of Homeland Security to develop a method for state, local, tribal and territorial governments to determine their High Value Assets (HVAs) to better focus their cybersecurity efforts where they are most needed. The CIAS is developing guidance based on best practices to address the identification, categorization and prioritization of IT systems to enable increased protection of HVAs across various jurisdictions. This includes the development of scalable guidelines, templates and tools that can be used to facilitate implementation of identified processes within the context of each community's risk management framework, available resources and authorities.

Papers Presented at HICSS and IEEE

White, Sjelin, Harrison, "The Need for Information Sharing and Analysis Organizations to Combat Attacks on State and Community Public and Private Networks", 52nd Annual Hawaii International Conference on Systems Science, January 9, 2019, Grand Wailea, Maui, HI

Harrison, Rutherford, White, "The Honey Community: Use of Combined Organizational Data for Community Protection", Proceedings of the 48th Annual Hawaii International Conference on System Science, January 5-8, 2015, Grand Hyatt, Kauai, Hawaii

Harrison and White, "Information Sharing Requirements and Framework for Community Cyber Incident Detection and Response", 2012 IEEE International Conference on Technologies for Homeland Security, 13-15 November 2012, Waltham, MA.

Zhao and White, "A Collaborative Information Sharing Framework for Community Cyber Security", 2012 IEEE International Conference on Technologies for Homeland Security, 13-15 November 2012, Waltham, MA.

White, "The Community Cyber Security Maturity Model", 2011 IEEE International Conference on Technologies for Homeland Security, Waltham, MA, November 15-17, 2011.

Granado and White, "Developing a Community Cyber Security Incident Response Capability", 42nd Annual Hawaii International Conference on System Sciences, 5-8 January 2009, Big Island, Hawaii.

EXERCISES & TRAINING

SEPT 13 2002 DARK SCREEN: First city tabletop exercise in San Antonio

MARCH 6 2003 1st ISAC EXERCISE: Financial Services ISAC, New York City, NY

FEB 6-10 2006 CYBER STORM: CIAS participates in DHS cybersecurity exercise

OCTOBER 2007 OPERATION WEBLOCK: Joint effort with Florida dept. of law enforcement

OCT 24-26 2018 First CyberAcademy class in the United Kingdom (with Raytheon)

NOV 4-8 2018 First CyberAcademy class in Kuwait (with Raytheon)

2002-2014

CIAS works with initial 5 states as community program established

California
Texas
Delaware
Illinois
N. Carolina

FEB 21-24 2016

First Cyber Academy class in the UAE (with Raytheon)

"The CIAS looks forward to continuing to develop critically needed training for states, locals, tribes and territories, as well as organizations within communities. We will focus on dynamic and relevant topics that focus on new trends and issues to stay on the cutting edge of training and exercises."

~ Natalie Sjelin, Associate Director – Training

Information Security Training

The CIAS has developed and delivered high-quality, high-impact cybersecurity training courses, seminars and workshops since 2004. A variety of cybersecurity initiatives are provided to better prepare the workforce, information technology professionals, organizations and communities. Courses are both technical and non-technical to address all cybersecurity training needs.

These courses are focused on improving overall cybersecurity awareness, technical capabilities, professional development, processes and continuity plans. In addition, courses assist community and state leaders to prevent, detect, respond to and recover from cybersecurity incidents.

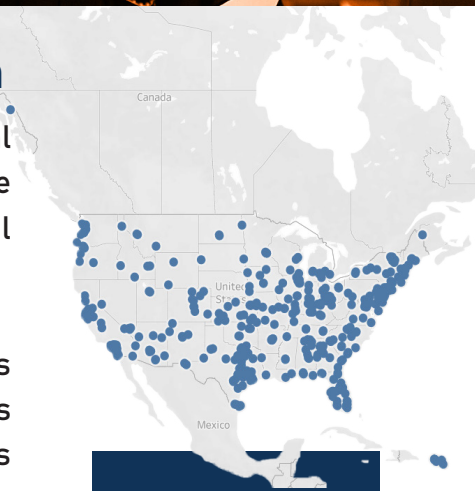
National Cybersecurity Preparedness Consortium

In 2013, to fill the cybersecurity preparedness training and technical assistance gap and to increase cybersecurity preparedness throughout the nation, UTSA partnered with four other universities to establish the National Cybersecurity Preparedness Consortium (NCPC).

The concept of the consortium is that cybersecurity is everyone's responsibility. In partnership with DHS/FEMA, the consortium members deliver online and face-to-face training and technical assistance, which is based on the CIAS' Community Cyber Security Maturity Model (CCSMM).

The NCPC Partner Organizations:

Norwich Pro™ · The University of Memphis, Center for Information Assurance · Texas A&M Engineering Extension Service · CIAS, Center for Infrastructure Assurance and Security · University of Arkansas System, Criminal Justice Institute



107,861

NCPC participants trained as of October 2020

EXERCISES & TRAINING

In 2002, the CIAS held its first community exercise Dark Screen (pictured below) and has since conducted exercises in partnership with the U.S. Secret Service Electronic Crimes Task Forces and the Information Sharing and the Analysis Centers (ISAC). Additionally, the CIAS has participated in Cyber Storm national level exercises and developed online and instructor-led courses certified by the Federal Emergency Management Agency (FEMA).

4 FEMA Certified Courses Developed (2006-2012)

Certified by FEMA's National Training and Education Division, courses were delivered to 62 classes in 15 states. 1,400 participants were trained and the CIAS hosted 3 FEMA conferences.

3 Web-based FEMA Certified Courses Developed (2013-2016)

Available to all U.S. states, communities, tribes and territories, these courses have trained 300 participants since 2019 and are found in FEMA's National Catalog for First Responders.

14 Executive Leadership Courses for 198 Military Personnel

The CIAS developed and delivered an Executive Leadership Cybersecurity Training course for the Texas Air National Guard senior military personnel between October 2015 and July 2019.

80 Small Businesses Reached with Cybersecurity Training

In 2017, the CIAS developed and continues to deliver Small Business Cybersecuity Training in a partnership with the Small Business Development Center at UTSA.

3 Day Executive Leadership Course Goes International

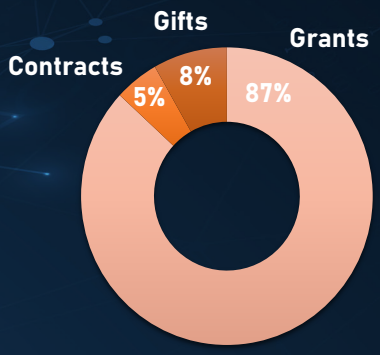
In 2018, an Executive Leadership Cybersecurity workshop was developed and delivered in Mexico City, Mexico, with UTSA's International Programs and Professional Development.

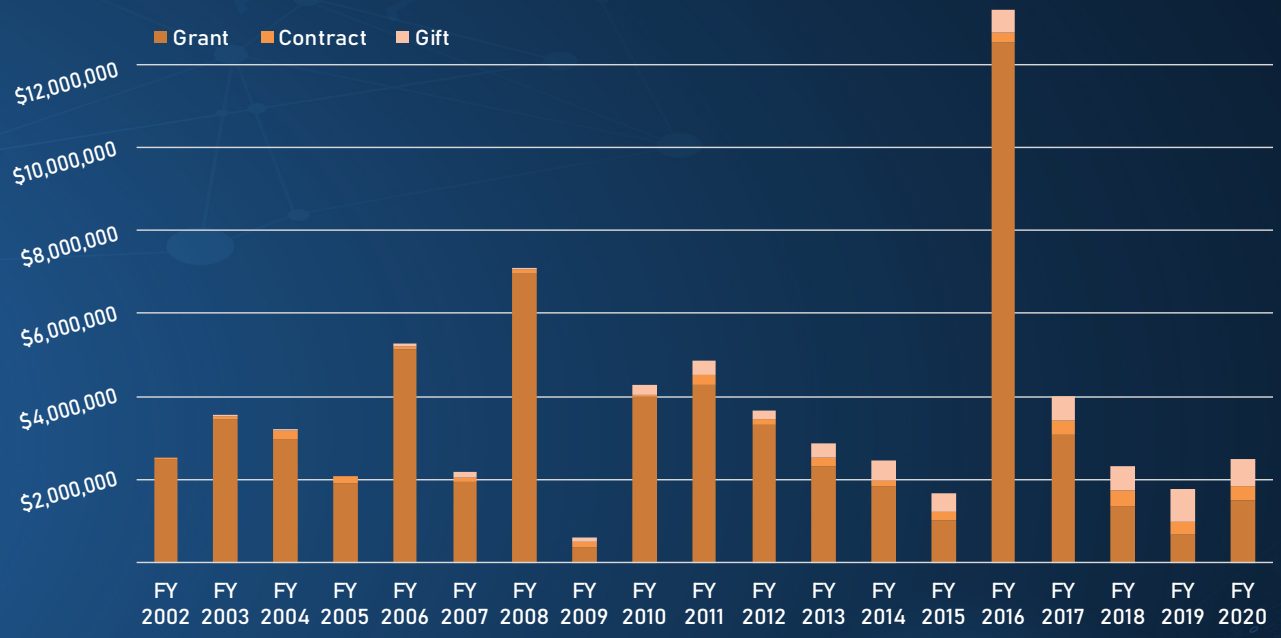
4 Certification Prep Courses Developed & Delivered

Since 2016, in partnership with UTSA's Extended Education, the CIAS has developed and deliverd annual certification prep courses for CISSP and CompTIA A+.

FINANCIAL IMPACT

CIAS Income (FY 2002-FY 2020)
$71,855,915.03

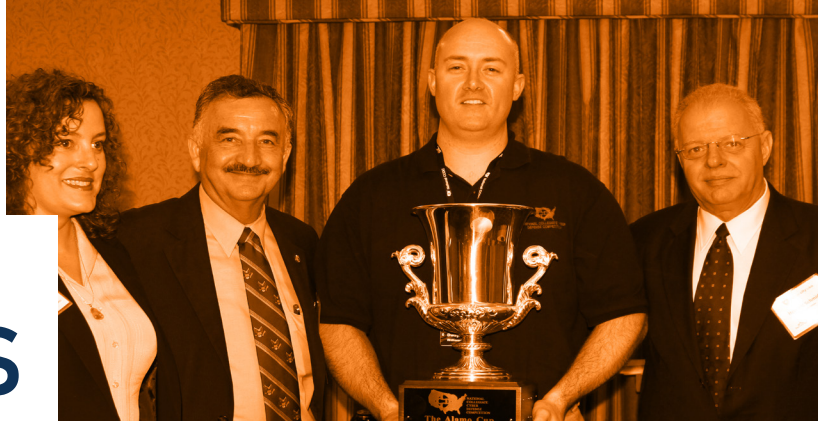




Total Revenue Awarded by the Top CIAS Program Supporters

As a non-profit center at UTSA, the CIAS has grown its information sharing initiatives, training and exercise services, cyber defense competitions and K-12 educational program thanks to sponsors, grants, gifts and contracts. The chart to the left provides a snapshot of the top 13 CIAS supporters through June 2021.

Cyber Defense COMPETITIONS



April 15-17, 2005
1st Collegiate Cyber Defense Competiton (CCDC) is held

Feb. 11, 2006
1st high school cyber defense competiton held (precursor to CyberPatirot)

April 21-23, 2006
1st National CCDC event held in San Antonio, Texas

2009
1st AFA CyberPatriot competition held in Orlando, Florida

Oct. 15, 2011
1st Panoply event held for college students

2011
NCCDC participation surpasses 1,000 students!

The CIAS is a pioneer and global leader in cybersecurity competitions.

Since 2005, the CIAS has been developing and conducting competition programs to help educate, train and prepare individuals for the information assurance workforce.

The CIAS has been recognized for its competition efforts in the Presidential Cyberspace Policy Review and by the 111th Congress in House Resolution 1244. In 2011, the CIAS was awarded the inaugural "Leadership in Security" award from Visa for work on the Collegiate Cyber Defense Competition Program.

The CIAS is currently involved in four competition programs: The Collegiate Cyber Defense Competition, Panoply, CyberPatriot and Hivestorm.

Pictured top to bottom: Dwayne Williams holding the NCCDC Alamo Cup during a 2010 tour with sponsors; 2013 CyberPatriot Team; 2018 NCCDC team; 2018 NCCDC Champions UVA.

Competitions are an ideal tool for training and developing the cyber workforce. They test knowledge and hands-on skills through experiences you can't get in any other setting."

~ Dwayne Williams, Associate Director, Technology, Research & Cyber Competitions

Aug. 15, 2018
1st eSentinel competition held virtually for U.S. schools

2019
NCCDC participation surpasses 3,600 students!

Nov. 1-2, 2019
1st Hivestorm competition is held

The CIAS flagship competition, the Collegiate Cyber Defense Competition, was inspired by a National Science Foundation sponsored meeting where attendees expressed a strong desire to have a way to gauge the practical experience and cyber security skillsets of students in colleges.

National Collegiate Cyber Defense Competition (NCCDC)

The Collegiate Cyber Defense Competition (CCDC) system was the first cybersecurity competition focused on the operational aspect of managing and protecting an existing small business network infrastructure.

CCDC allows teams of undergraduate and graduate students at colleges and universities across the United States to exercise their academic and technical education in a business oriented, defensive information assurance competition. CCDC is a tiered competition with qualifying and regional events leading to a national championship.

The CCDC events are an excellent opportunity for students to gain practical, hands-on experience in cyber security and information technology allowing them to expand their educations beyond the traditional classroom environment. CCDC fosters development of technical, leadership and teamwork skills highly prized by government and industry. Most CCDC events include a recruiting event to facilitate student and potential employer networking.

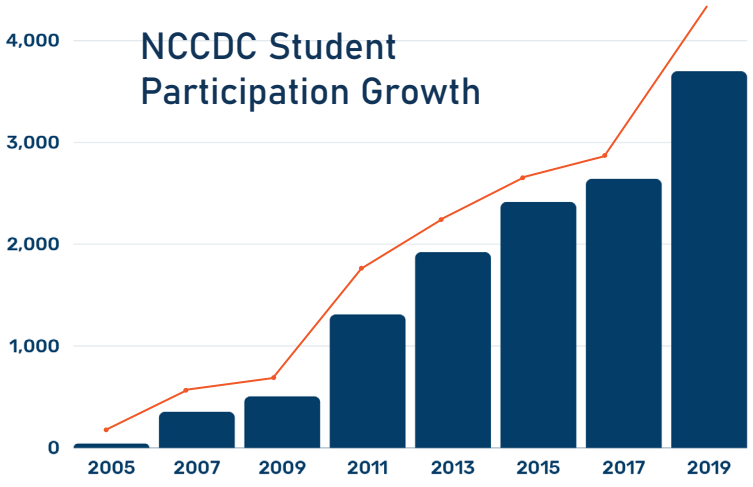
Impact of the CCDC NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

Influenced Curriculum and Industry/ Academia/Gov't Partnerships
Universities now provide more practical hands-on practice and experience

Propagates Success, Dissemination of Knowledge and Mentorship

Used as a Testbed for New and Emerging Technologies from Partnering Companies

NCCDC Student Participation Growth



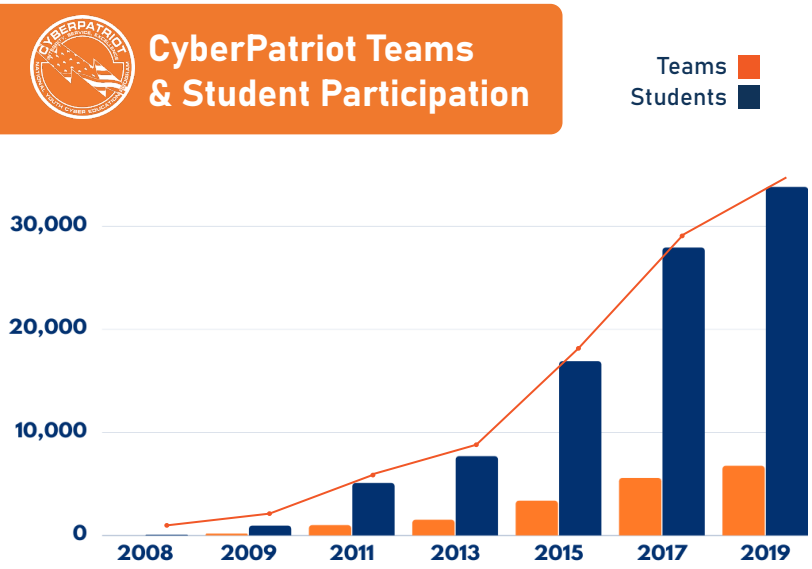
Cyber Defense COMPETITIONS

CyberPatriot Program

In 2009, partnering with the U.S. Air Force, Air Force Association (AFA) and SAIC, **the CIAS co-founded CyberPatriot**, the world's largest cyber defense competition and the AFA's National Youth Cyber Education Program.

The competition's purpose and design are to inspire students toward careers in cybersecurity or other science, technology, engineering and mathematics (STEM) disciplines. The CIAS designs, builds and supplies the technology and virtual machines used in the CyberPatriot Cyber Defense Competition component of the program. CIAS personnel support the online competitions and National Finals components of the CyberPatriot program.

CyberPatriot Teams & Student Participation



By 2012, CyberPatriot had outgrown its original competition system. Well over 1,000 teams were participating and a new competition system was needed. The team at the CIAS were asked to develop a competition system that could easily scale to a large number of teams. The CIAS team, led by Dr. Keith Harrison, created the CyberPatriot Competition System (CCS), which is now used in all competition images. The CCS gives competitors near real-time scoring feedback and a public scoreboard, and by 2014 it was a full-up competition system using Windows and Linux-based systems. The system continues to keep pace with CyberPatriot's growing needs and the needs of sister competitions in Europe, Saudi Arabia, Australia and others.

CIAS has also played key roles in the development of AFA CyberCamp curriculum, the Elementary School Cyber Education Initiative modules and a promotional demo that allows prospective coaches and competitors to get the look and feel of the CyberPatriot competition without having to download any software or virtual images.

Panoply

The CIAS introduced the network security competition Panoply to the world at the 25th Security in Government Conference held in Canberra, Australia in 2013. A timed competition event for college students and industry professionals, Panoply can be conducted in-person or virtually.

Designed as network assessment and network defense competitions that are combined into a single event, Panoply challenges competitors to vie for control of common resources and the critical services on those resources.

Following the success of Panoply at ISC2 Security Congress and Blackhat (both in the U.S. and Europe) events, an international counterpart, eSentinel, was developed with funding and support by the Department of Homeland Security for international college students.

HiveStorm

Launched in 2019, HiveStorm is a collegiate-focused cyber defense competition. Teams of two-to-four players compete by securing provided Windows and Linux based virtual machines. Teams accumulate points for addressing each scored issue and must race against the clock to accumulate as many points as they can before time expires.

Hivestorm provides an excellent opportunity for teams to practice security, forensic, configuration and system administration tasks. The defensive and administration skills developed and exercised in Hivestorm help prepare students for other events such as our Collegiate Cyber Defense Competition or Panoply.

27 Number of countries where the CIAS has hosted competitions

187K* **COMPETITORS**

have participated in CIAS cyber defense competitions worldwide

**from 2005-2019*

K-12 CYBERSECURITY PROGRAM

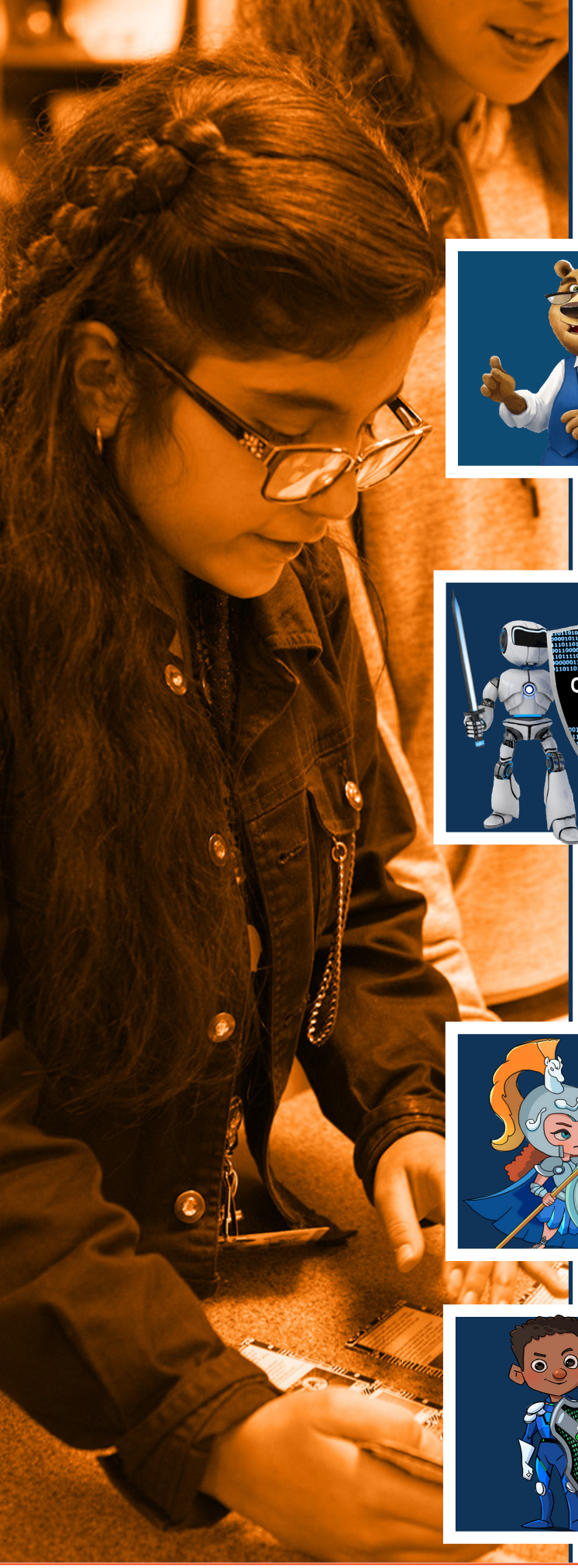
In 2015 the Air Force Association contracted with the CIAS to develop three digital games for its Elementary School Cyber Education Initiative (ISCEI): Security Showdown 2, Packet Protector and JeffOS. About the same time, Dr. White's 2013 National Science Foundation (NSF) Grant to produce a digital cybersecurity game to reach students in K-6 was coming to an end.

2019 Cyber Threat Defender Tournament Winners Pictured L-R: Second Place Winner Farah Alsmadi; First Place Winner Hamza Alsmadi; Third Place Winner Elyssa Ramos

Over the life of this grant, two prototype educational games were developed. The first being an interactive game, Project Cipher, which introduces students, in fourth grade and up, to cybersecurity principles that focus on cryptography. The second protype game, Pyramid of Knowledge, evolved into a testing tool for teachers. It is designed to provide educators with the ability to build their own quizzes for use in the game interface. These games launched the CIAS educational game effort.

Looking to create a Culture of Cybersecurity across the nation starting with students, the CIAS launched its K-12 Cybersecurity Program in 2016 with Cyber Threat Defender: the Collectible Card Game, which was designed to teach basic cybersecurity principles to students in grades 6-12.

The CIAS K-12 Cybersecurity Program currently consists of the following educational games: 1) Cyber Threat Defender: The Collectible Card Game; 2) Cyber Threat Defender Digital; 3) Cyber Threat Protector; 4) Cyber Threat Guardian; and 5) the CyBear Culture of Cybersecurity Program.



The K-12 Cybersecurity Toolbox

CyBear Culture of Cybersecurity

Centered around the CyBear family, the cybersecurity-focused family introduces children, primarily ages 5-11, to cybersecurity words and phrases, guides them through problem solving with puzzles, and engages them with interactive activities through a variety of free activity sheets and games.

Cyber Threat Defender (Grades 6+)

Released in 2016 and available as both a collectible card game and electronic download, CTD provides a basic awareness of a number of security issues. The card game, available in English and Spanish, is a fun, multi-player game in which players build their networks while defending against realistic cyber-attacks. It's used in middle- and high-school classrooms worldwide to provide awareness of security issues and techniques.

Cyber Threat Protector (Grades 3-5)

Released in 2020, this multi-player card game builds upon lessons learned in Cyber Threat Guardian. It strengthens knowledge on how to build a safe network and introduces strategies to defend against cyber threats.

Cyber Threat Guardian (Grades K-2)

Released in 2021, CTG is a multi-player card game that helps young players learn about cyber safety. It also begins to introduce the foundations of cybersecurity defense concepts and vocabulary.

K-12 CYBERSECURITY PROGRAM

The CIAS K-12 Cybersecurity Program is rooted in a 2013 NSF Grant that conducted research into developing age-appropriate games to help introduce cybersecurity and/or cyber safety knowledge to students in grades K-6. The research focused on two key areas: (1) engaging an important group in our nation regarding a cybersecurity workforce pipeline for the future and (2) creating a culture of security within the nation.

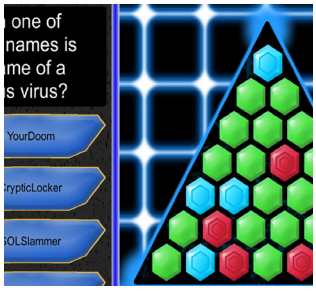
Now in 2021, the CIAS continues to work to fill an existing gap between students and careers in the cybersecurity workforce. The nation can no longer wait for students in college or university to decide that a cybersecurity field might be a possible career path. The CIAS K-12 program is reaching students at the earliest time to (1) create better cyber citizens and (2) help them to begin exploring the field of cyber as a possible career path."

- Larry Sjelin, Director of Game Development

Cybersecurity Tools & Resources

Project Cipher (Grades 4+)

Released in 2018, Project Cipher is used to introduce cybersecurity principles that focus on cryptography concepts. A digital game, Project Cipher is free to download and teaches techniques for encoding and decoding ciphers to either hide or discover information.



Pyramid of Knowledge (K-12 Educators)

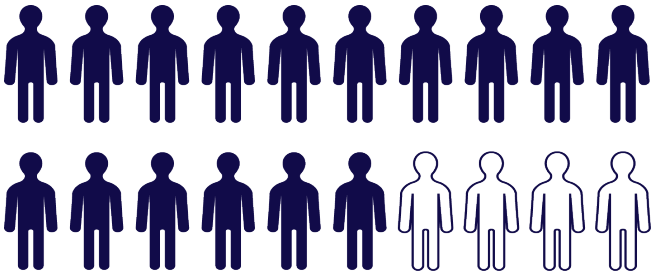
Released in 2018, Pyramid of Knowledge (PoK) is a testing tool that provides educators with the ability to build their own quizzes in a creative way. PoK also introduces students to cybersecurity principles through game play with its "Pyramid" quiz interface. This platform is designed to complement an educator's STEM program.

National Level Exercise

In 2019, the CIAS developed a cyber preparedness game for FEMA's 2020 National Level Exercise. The game focused on a community level cyber exercise in which a community faced a wide range of cyber-attacks and required each organization to build a response plan based upon the NIST framework.

MAKING AN IMPACT IN K-12 CYBERSECURITY EDUCATION*

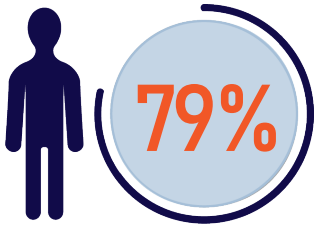
250,000 middle and high school students reached with Cyber Threat Defender



80% of players have an increased interest in cybersecurity fields after playing

50K Card decks distributed across the U.S.

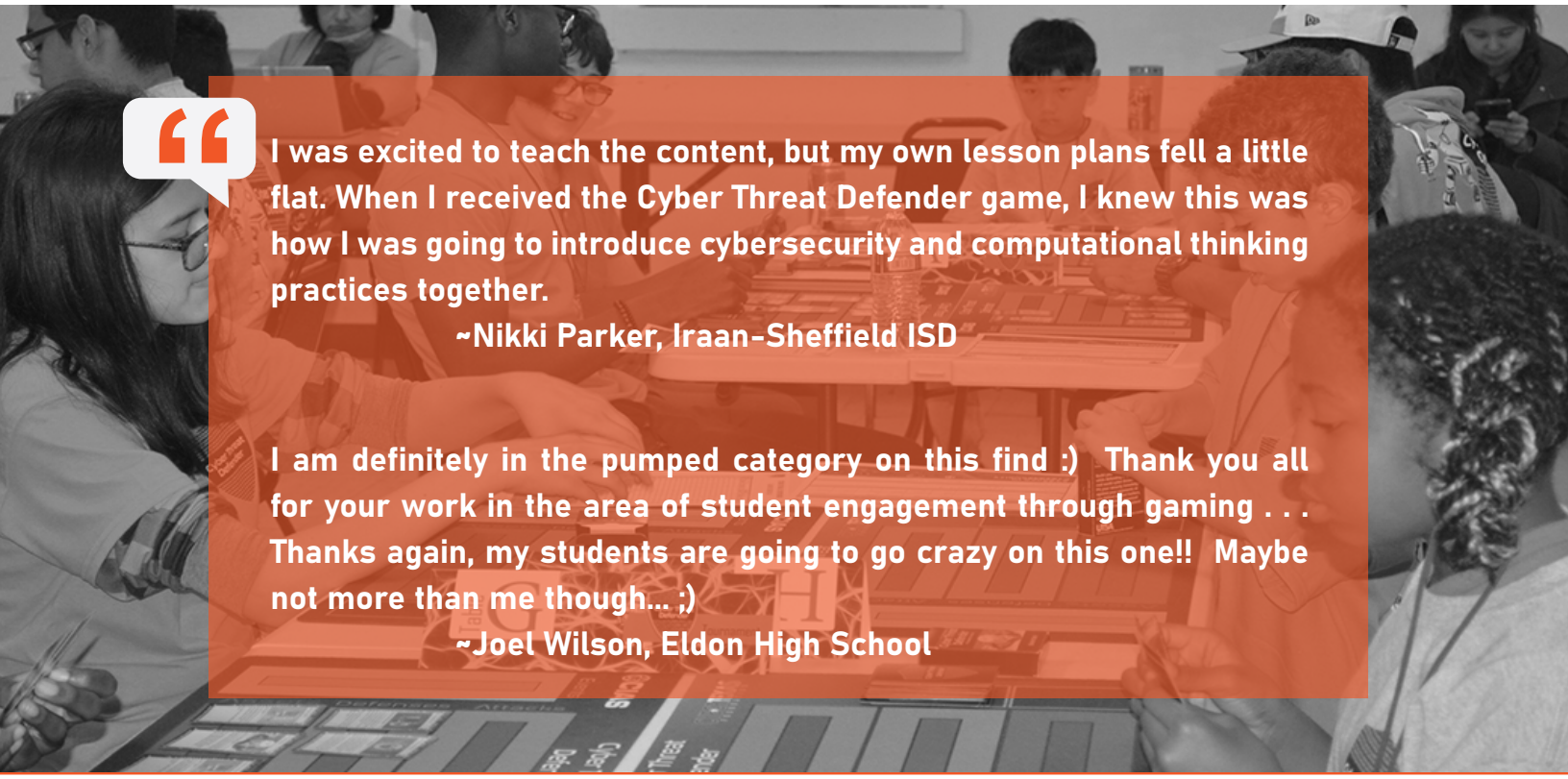
7,500K Downloads of Cyber Threat Defender



79% Cybersecurity knowledge improved after playing games

51% Percent of players that have applied what they've learned in their daily life

*Stats as of April 2021



"I was excited to teach the content, but my own lesson plans fell a little flat. When I received the Cyber Threat Defender game, I knew this was how I was going to introduce cybersecurity and computational thinking practices together.

~Nikki Parker, Iraan-Sheffield ISD

I am definitely in the pumped category on this find :) Thank you all for your work in the area of student engagement through gaming . . . Thanks again, my students are going to go crazy on this one!! Maybe not more than me though... ;)

~Joel Wilson, Eldon High School

INFORMATION SHARING

Information Sharing and Analysis Organization (ISAO) Standards Organization

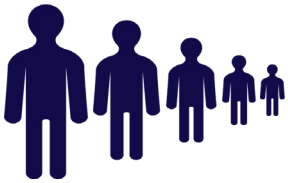
In October 2015, The U.S. Department of Homeland Security selected a team, originally led by UTSA, LMI and R-CISC, as its Information Sharing and Analysis Organization Standards Organization (ISAO SO). Through an executive order in February 2015, the ISAO SO was tasked with developing standards and guidelines for the creation of and collaboration between ISAOs.

The CIAS continues to lead the ISAO Standards Organization's industry, academia and government volunteers in developing cybersecurity information sharing guidelines. ISAOs continue to play an integral role to national efforts to promote secure, rapid and widespread information sharing that helps organizations detect and block increasingly sophisticated cyber security threats.

The ISAO SO works with existing information sharing organizations, owners and operators of critical infrastructure, relevant agencies and other public- and private-sector stakeholders through a voluntary consensus standards development process to identify a common set of voluntary guidelines for the creation and functioning of ISAOs. These guidelines address, but are not limited to, contractual agreements, business processes, operating procedures, technical specifications and privacy protections.

13
No. of ISAO SO Documents Published from 2015-2020

79 No. of information sharing organizations registered on ISAO.org as of April 2021



Pictured Left: CIAS team representing the ISAO SO at a RSA Conference.
Pictured Top: ISAO SO roundtable event.

Texas ISAO

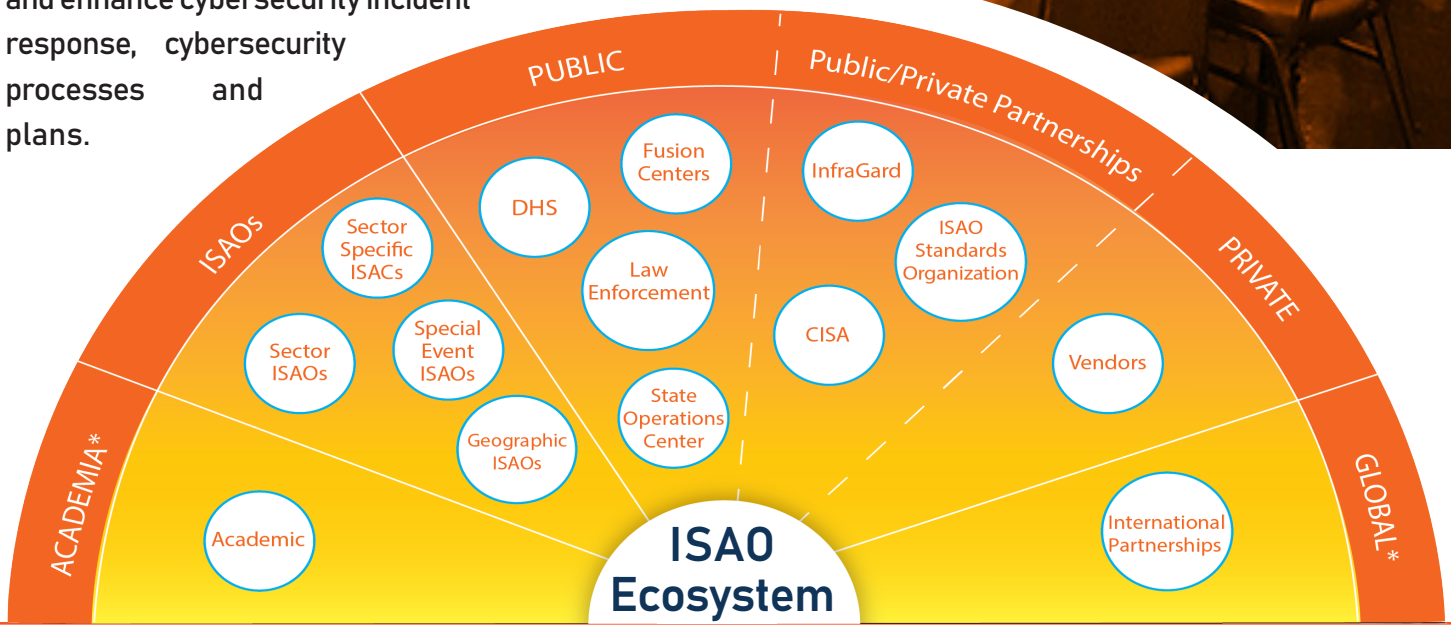
In 2019, the Texas Legislature called for the creation of an ISAO to provide a forum for state agencies, local governments, public and private institutions of higher education, and the private sector to share information regarding cybersecurity threats, best practices and remediation strategies.

The Texas ISAO (TxISAO) came into existence as a loose collection of entities working together to help improve security around the state. The CIAS was selected to represent UTSA's contribution as one of the founding members of the ISAO. The CIAS is responsible for assisting the membership with education and awareness to promote preparation, protection and prevention.

CIAS-ISAO

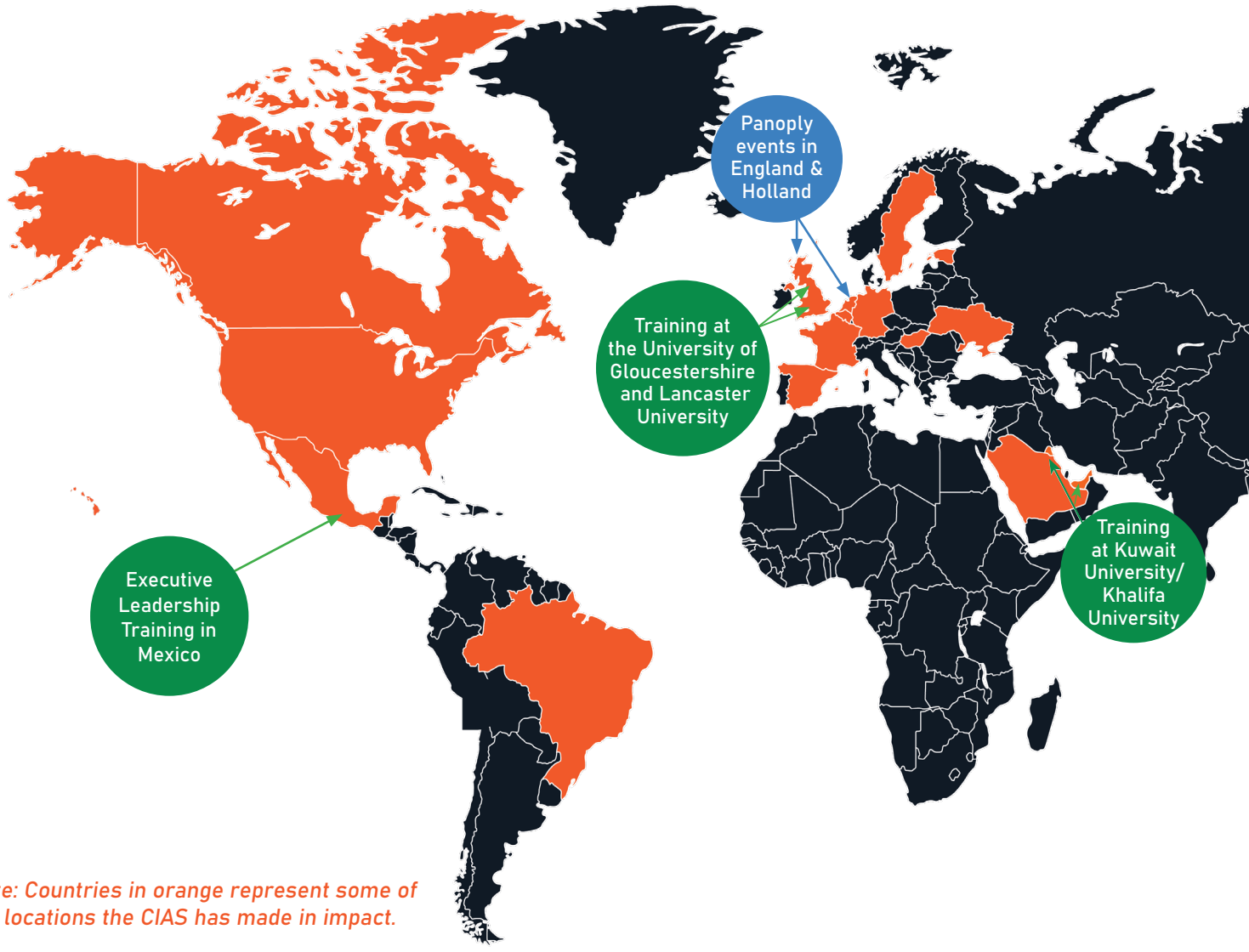
The core mission of the CIAS-ISAO is to help states, tribes, local jurisdictions and territories to establish a comprehensive cybersecurity program by using the congressional-supported Community Cyber Security Maturity Model (CCSMM).

Launched in 2020, the CIAS-ISAO membership is made up of both industry and government entities. The CIAS-ISAO also helps geographically-based communities to establish or enhance their ISAOs, create a trusted community environment, provides a roadmap based on the NIST Cyber Security Framework, and conducts assessments to validate and enhance cybersecurity incident response, cybersecurity processes and plans.



GLOBAL IMPACT

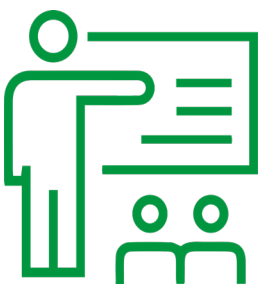
The CIAS continues to enforce the concepts of protecting essential cyber and physical assets while improving information gathering and sharing initiatives. Through interactive training sessions, cyber defense competition events and K-12 cybersecurity education, the cybersecurity posture of local communities, states and even the nation are strengthened.



Note: Countries in orange represent some of the locations the CIAS has made in impact.

Gaming

The Cyber Threat trilogy of games have been distributed to educators and professionals in 17 countries as of 2020



Training

Cybersecurity academies have been conducted in the U.K. and Middle East, as well as leadership training in Mexico.

Below is a snapshot of how the CIAS is taking a global approach to creating a culture of cybersecurity with all ages, backgrounds and experience.

Competitions

Various cyber defense competitions have been hosted in 27 countries, from the United Kingdom to Singapore.

Thank You to the Organizations* that have Helped the CIAS Make an Impact!

FEDERAL

780th Military Intelligence Brigade
Air Force Civilian Service
Central Intelligence Agency (CIA) AUS
Cybersecurity & Infrastructure Security Agency
Department of Defense
Department of Energy
Department of Homeland Security
Federal Bureau of Investigation
Federal Emergency Management Agency
National Security Agency
SPAWAR Atlantic
US Air Force
US Air Force Reserve
US Army Reserves
United States Secret Service

PRIVATE INDUSTRY

ABS Global Trading Limited
Accenture
Air Force Association
Amazon
AT&T
Boeing
Cisco
CyberTexas Foundation
Deloitte
Facebook
FireEye
General Dynamics
IBM
Juniper
KPMG
Lockheed Martin
Microsoft
MITRE Corporation
OpenVPN
Palo Alto Networks
Rackspace
Randori
Raytheon Intelligence & Space
SAIC
Southwest Airlines
Splunk
Uber
Walmart Global Tech

PROFESSIONAL ORGANIZATIONS

Black Hat
ISC2
ISSA

ACADEMIA

Carnegie Mellon University
Norwich University
Texas A&M
University of Arkansas
University of Memphis
University of Texas

INTERNATIONAL

AusCERT (Australian CERT)
The Netherlands Organization (TNO)

not a comprehensive list


CIAS