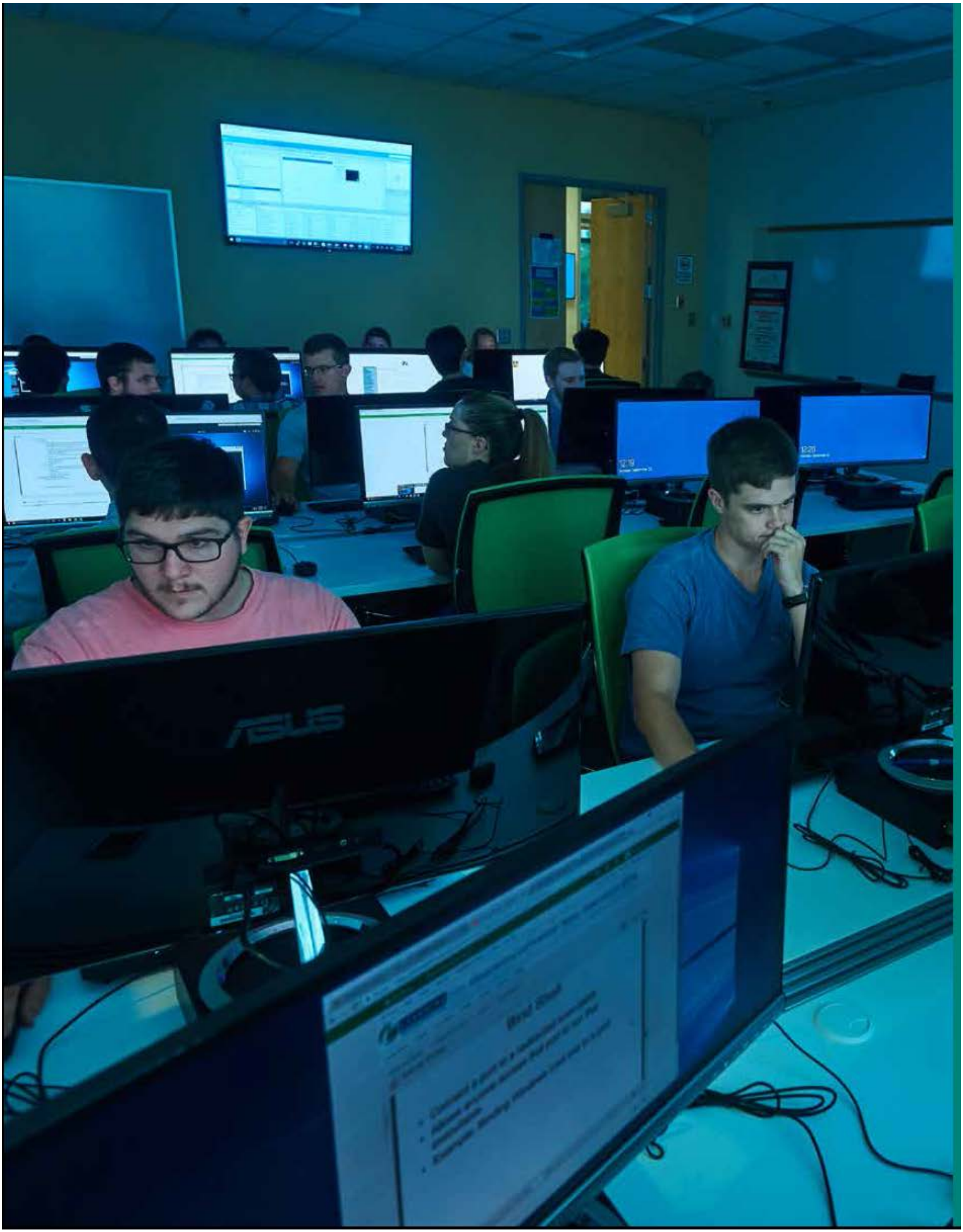
PENSACOLA CYBER COAST

Live Coastal. Work Cyber.

A Cybersecurity Strategic Plan Report

Developed for:
FloridaWest Economic Development Alliance
and the
Pensacola Cybersecurity Community

Prepared by:
Innovation Strategies, LLC, Janet Woolman, M.L.I.S.
Gulf Breeze, Florida
Jeanne Daboval, D.B.A.; William Dees, Ph.D.; and Lyle Hardee, M.S.
Lake Charles, Louisiana


ASUS

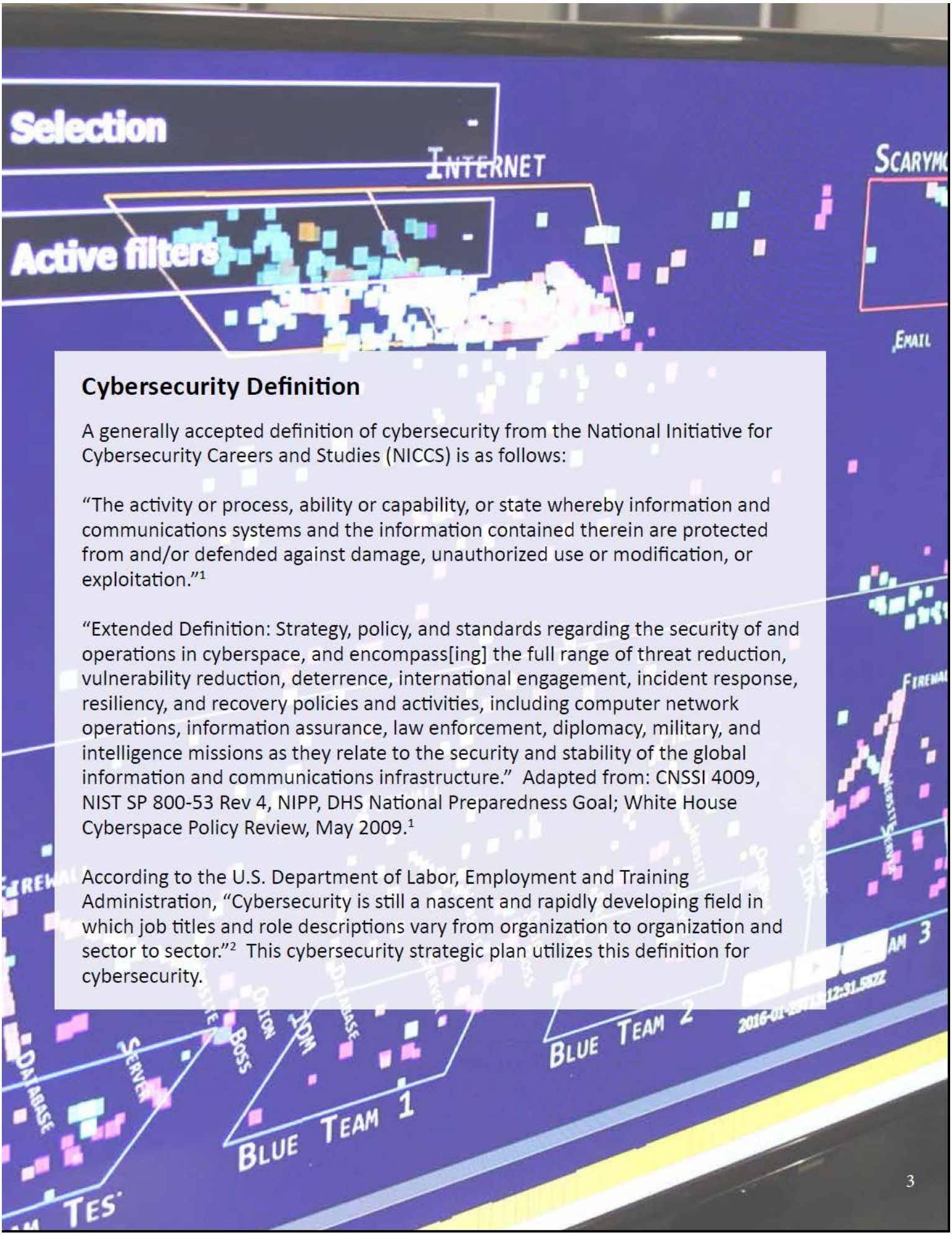
CONTENTS

Statement from the Nation's First US Chief Information Security Officer

Cybersecurity is a worldwide risk management issue. In today's digitally connected world, nearly every aspect of modern life relies on digital technologies that power innovation and our sharing of knowledge, fuel our national economy, and preserve our national security. Pensacola, Escambia County, and the Gulf Coast region have the unique opportunity to create the world's best public and private sector cyber partnership, making the "Cyber Coast" a recognized world leader in cybersecurity. With a national deficit of skilled cyber professionals estimated at over one million personnel (and rising every day), the Cyber Coast can accelerate its emphasis on programs in science, technology, engineering, the arts and mathematics (STEAM) from K-12, at the university level, and into continuing education and retraining programs. The result will be creation of the best and most cyber-aware community and recognition as a coveted source of the world's cyber leaders. The region's industry is already heavily invested in information technology and digital operational technology. By cyber-hardening critical infrastructure and industrial control systems, industry and public entities can better work together to grow a more robust and competitive economy that serves the community well and attracts more businesses to the region. Making the Cyber Coast a recognized cybersecurity leader will not be easy. Government, industry, academia, and the citizens of the region must form a team to achieve the strategic goal. I am confident with its strong, smart, and hard-working people; bountiful resources; and drive for excellence that the Cyber Coast is well on its way to vaulting to national prominence.

GREGORY J. TOUHILL, CISSP, CISM
Brigadier General, USAF (ret)
First US Chief Information Security Officer (2016-2017)

Image Source: http://www.af.mil/About-Us/Biographies/Display/Article/108360/brigadier-general-gregory-j-touhill/



Cybersecurity Definition

A generally accepted definition of cybersecurity from the National Initiative for Cybersecurity Careers and Studies (NICCS) is as follows:

"The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."[1]

"Extended Definition: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure." Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009.[1]

According to the U.S. Department of Labor, Employment and Training Administration, "Cybersecurity is still a nascent and rapidly developing field in which job titles and role descriptions vary from organization to organization and sector to sector."[2] This cybersecurity strategic plan utilizes this definition for cybersecurity.

NATIONAL STATUS OF CYBERSECURITY

"Here in the upside of Florida, our cybersecurity professionals are shining a light on a dark cyber underworld that increasingly threatens our information, infrastructure and digital communications."

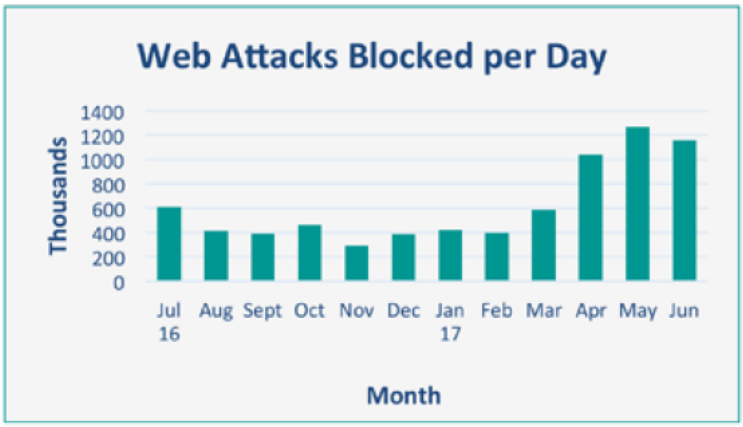
"Since Tristan de Luna sailed into Pensacola Bay in 1559 and set his encampment, Florida's life, welfare, borders and riches have been coveted by many enemies. Today, the enemy still exists, although their face has changed. We no longer see the enemy who wishes to harm or steal our livelihoods. They operate in the digital world. Thankfully, local cybersecurity experts understand this threat and are continually training and operating in the domain of cyberspace."

"Florida is not only a beautiful place to live or retire. With the cyber-security threat on the rise, the demand for people who can defend our networks is growing rapidly. Florida is home to some of the best educational institutions, where students are learning how to cope with the dangers in the new world of cybersecurity. Florida also remains home to some of the best cybersecurity operators in the business, whether they are operating within the Department of Homeland Security or the Department of Defense."

Bill Dunn,
Vice President
Operations
Metova CyberCENTS

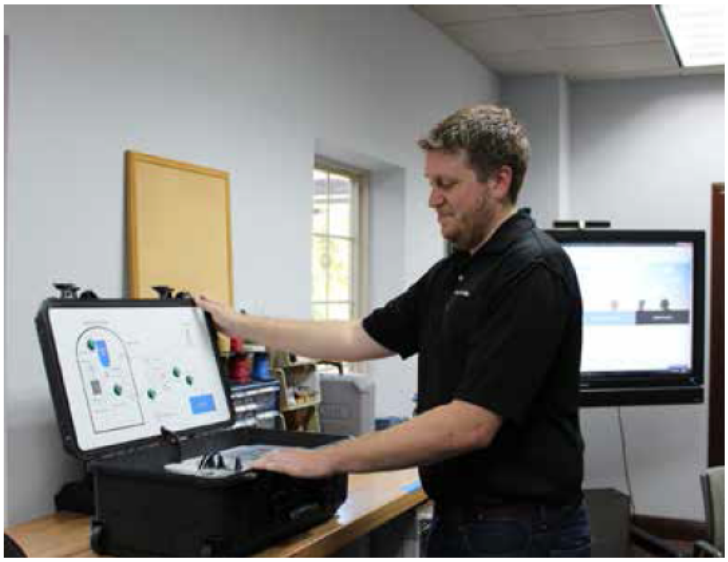
In today's technology-connected world, effective cybersecurity practices are imperative to protect and manage information, networks, technology, and infrastructure. Cybersecurity operations must be integrated into all business and local government processes. Effective risk management includes an investment in cybersecurity designed to protect competitive advantages, assets, and infrastructure. Cybersecurity is most effective when all levels of government in partnership with the private sector employ appropriate policies and practices.[3]

"Cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015." (Cybersecurity Ventures)



Source: Symantec security response

"The cybersecurity workforce shortage is projected to reach 1.8 million by 2022." ((ISC)²)



Metova CyberCENTS

"Global cybersecurity spending will exceed $1 trillion by 2021." (Cybersecurity Ventures)


NAVY FEDERAL
CREDIT UNION

EXECUTIVE SUMMARY

Pensacola has a unique opportunity to become a regional and national leader in cybersecurity. The FloridaWest Economic Development Alliance comprises public and private entities dedicated to advancing the economic health and vitality of the region. FloridaWest, on behalf of the cybersecurity stakeholder community, retained Innovation Strategies, LLC to develop a cybersecurity strategic plan. This plan will build a strong workforce, identify education and career pathways, and enhance the economic and community impact of cybersecurity in northwest Florida.

The proposed cybersecurity strategic plan emphasizes the competitive advantages of Pensacola, outlines needs and opportunities, inventories capacity, and offers four goals and multiple broad strategies to grow the cybersecurity industry.

The four goals of "Live Coastal. Work Cyber." are:

1. Build a thriving cybersecurity workforce
2. Strengthen partnerships to enhance cybersecurity innovation and economic development
3. Enhance technology infrastructure and optimize cybersecurity business climate
4. Market the Pensacola region's "Live Coastal. Work Cyber." brand

To become a trusted source of cybersecurity expertise and innovation, Pensacola must build upon and promote cybersecurity resources, programs, and networks in the region. Creating systems for cooperation and information sharing, developing targeted programs and resources to assist participating businesses, and facilitating entrepreneurship and innovation will strengthen the cybersecurity ecosystem.

The result of this work led to the vision of "Live Coastal. Work Cyber." which will make Pensacola's Cyber Coast the choice place to live and perform cybersecurity work. The mission is to "Lead as the Nation's trusted provider for cybersecurity operations, expertise, and innovation."

Note: This document is intended to serve as: (1) a path for developing the Pensacola cybersecurity community and industry and (2) a flexible dynamic plan that will change and evolve as new information becomes available.

PROJECT OVERVIEW

Benchmarked cybersecurity communities. Source: https://mapchart.net

In January 2017, Innovation Strategies, LLC (IS) began working with FloridaWest and the FloridaWest Cybersecurity Advisory Group on behalf of the cybersecurity community to develop a strategic plan. This group is comprised of individuals from non-profit, for-profit, higher education, government, and military sectors. IS focused on the Pensacola-Ferry Pass-Brent Metropolitan Statistical Area (MSA) and other relevant areas to ensure the information collected represents a cross section of the cybersecurity community (Fig. 1). The IS principal conducted interviews, research, and data mining to determine drivers for short and long term strategies that will develop the cybersecurity industry in the Pensacola MSA. Starting with basic questions and stakeholder input, a roadmap for improving the cybersecurity landscape in Pensacola was developed.

PROJECT OVERVIEW (cont.)

Figure 1. Pensacola MSA. Source: http://www.floridasgreatnorthwest.com/regional-overview/msa-information/pensacola-msa.aspx

This plan builds on information from:

- 15+ local reports and studies;
- Prager Schneider Site Selection Perspective Assessment;
- Approximately 30+ interviews with cybersecurity federal and commercial executives, cybersecurity educators, workforce developers, cybersecurity entrepreneurs, cybersecurity workers, entrepreneurial and economic development professionals, cybersecurity military personnel, and civic leaders;
- Intelligence, market information, legislation - Florida Statutes (s. 20.61 F.S.; s.282.318 F.S.; s.282.0051 F.S.);
- Cybersecurity-based Frameworks (Baldridge, National Institute of Standards and Technology-National Initiative For Cybersecurity Education [and Workforce Framework], NIST Framework for Improving Critical Infrastructure Cybersecurity); and
- Cybersecurity stakeholder input gathering from a public strategic vision planning session (Appendix A in the Cybersecurity Strategic Plan).

CURRENT SITUATION

Pensacola's Cyber Coast is the nation's oldest trusted source for cybersecurity training and expertise. With its many resources, including Naval Air Station Pensacola and its numerous commands, private IT/cyber sector, and cybersecurity public sector, Pensacola offers partnership and business growth opportunities, balanced lifestyle choices, and an innovation ecosystem. Building on NAS Pensacola Corry Station's reputation as the "cradle of cryptology," Pensacola is well positioned to grow cybersecurity capabilities by leveraging innovation, enhancing public-private partnerships, and cultivating a workforce to support a complete cyber ecosystem.

"The Pensacola cyber industry is exploding The work is exciting; the mission is relevant; the technologies are cutting edge!"

"Pensacola cyber industry growth and shortage of skilled experts is creating opportunities unlike anywhere else. The work is exciting and it is on the beach!"

"The Pensacola cyber industry is growing fast! The community is incredibly supportive, opportunities abound and the region offers abundant natural and cultural resources attracting talent worldwide."

"The cyber work being done in Pensacola and the panhandle has national security relevance with Federal interagency, state and industry employment and research opportunities."

Sean O'Brien,
CSRA NETC ITSS
Program Executive

CHALLENGES

Sectors of the Pensacola cyber economy have evolved in a fragmented manner that is common for many emerging industries. For example, cybersecurity emerged to defend and protect information and information systems. Federal agencies required trained personnel to operate technology and secure information and infrastructure in new ways. To address cyber needs, Pensacola's federal missions changed, technology and government contracting companies offered different solutions, education providers offered new curricula, and business interactions and communications increased. Understanding the segmentation of the local cybersecurity ecosystem assists with developing solutions to improve organizational cooperation, infrastructure, and support for a strong cyber economy.

Cultivating an integrated cybersecurity workforce that is globally competitive and retained is a complex challenge. Cutting-edge cybersecurity education, training exercises, and professional development are necessary to generate a continuous cyber workforce pipeline. Education and training must be available from early childhood throughout life. Continual hardening of the workforce, advancement opportunities, practice and special resources are central to recruiting and retaining qualified professionals.

"The region is home to more than 500 companies and many industries including advanced manufacturing, information technology, cybersecurity, aerospace and defense, and government contracting. With award-winning IT/ cyber companies and corporations located in the Pensacola area, there is much opportunity for growth and innovation."

Michelle L. Taylor, Ed.D.,
Workforce Education Director
Escambia County School District

"A 2015 U.S. study found that African-Americans, Asians and Hispanics represent less than 12% of information security analyst positions combined, with females representing only 10% of the cybersecurity workforce."
(International Consortium of Minority Cybersecurity Professionals)

Pensacola needs a cohesive critical mass of commercial companies to grow the cyber industry. To build a critical mass, Pensacola's stakeholders need to formalize dialogue about workforce issues, prioritize resources available to assist existing companies, and focus on attracting new businesses and talent. Marketing the advantages of living and working in northwest Florida is paramount to the area's economic success.

The strong military presence and prevalent cybersecurity expertise is a dominant economic driver in the Pensacola area. The guarded nature of cyber work combined with restricted information sharing creates a challenge for innovation and opportunity sharing. The benefits and intellectual capital of a military ecosystem should be leveraged for economic growth in the cybersecurity industry.

"The cybersecurity program here at UWF lays an amazing groundwork for anything you want to do that's computer related, especially cybersecurity," Harper said. "It gives you all of these skill sets to do whatever you want to do in the field. You have courses like Cyber War Gaming and Ethical Hacking and Penetration Testing. Those are real, big-world topics that you think about when you think cybersecurity."

Gage Harper, UWF cybersecurity senior interested in government contract work after graduation

The cybersecurity workforce shortage is projected to reach 1.8 million by 2022 $(ISC)^2$ and Booz/Allen/Hamilton).

Centaur and Einstein

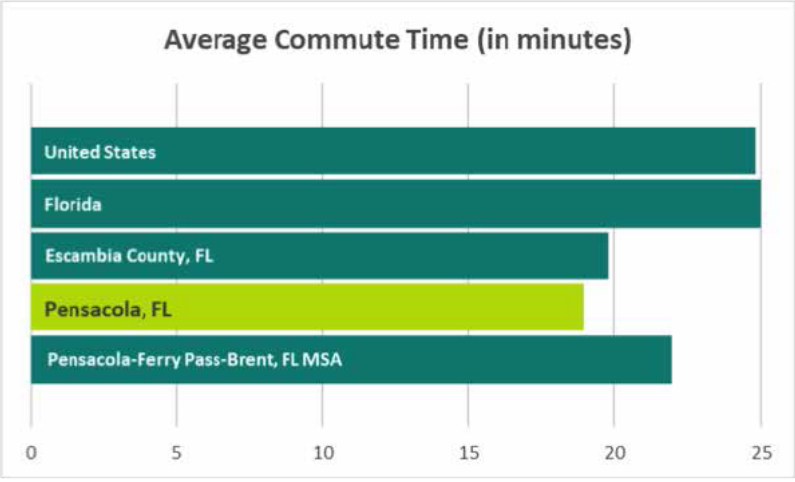
In 1998, the Department of Defense (DoD) created the Joint Task Force-Computer Network Defense (JTF-CND) under the U.S. Space Command in response to a growing cyber threat. In 1999, the Space and Naval Warfare Systems Command (SPAWAR) Pensacola office, tasked by the Defense Information Systems Agency (DISA) developed a pilot program (Centaur) to track Netflow data and help DoD better understand Non-Secure Internet Protocol Router Network (NIPRNet) usage. The Centaur system maintains a repository of detailed data regarding network traffic handled by the border and backbone routers on the NIPRNet.

JTF-CND became the Joint Task Force-Global Network Operations (JTF-GNO) and was reorganized under the United States Strategic Command. JTF-GNO assumed the responsibility for directing the operation and defense of the Global Information Grid and later integrated into the U.S. Cyber Command. With close ties to DISA, JTF-GNO understood the tremendous value that the Centaur pilot program could provide to the collective defense of the Department of Defense Information Network (DODIN). Within a few short years, the joint team of DISA, SPAWAR and JTF-GNO had transformed the Centaur program into one of the largest and most robust Netflow clusters in the world (containing up to 18 months of online related cybersecurity data). DHS was created in 2002, and the National Protection and Programs Directorate (NPPD) was established in 2007. A few of DISA's cybersecurity leaders helped establish the Department of Homeland Security's NPPD. These leaders possessed knowledge and expertise gained through the SPAWAR, DISA, and JTF-GNO collaboration that had produced the successful Pensacola-based Centaur program.

The University of West Florida is one of only six NSA/DHS CAE Cybersecurity regional hubs across the country.

Building on this success, DHS worked with SPAWAR Pensacola for initial creation of the sister program to Centaur-the Einstein program. Both DISA and DHS have a presence in Pensacola, which enables support and retention of institutional knowledge. In 2009, DISA increased Centaur program capabilities in a joint effort with NSA to better enable the "defense of the DODIN" mission. This effort created an environment in which cybersecurity data from systems located through the DODIN could be consolidated into one environment. These capabilities provided a global view of traffic on the DODIN and helped support detection and response of anomalous behavior linked to Advanced Persistent Threats (APTs).

In 2012, DISA expanded the Einstein program, added cloud computing capabilities, renamed it "Acropolis," and designated the DISA Pensacola team (now called Centaur Operations) as the sole management group for all Acropolis tools and capabilities.[4-19]



Pensacola commute time.
Source: https://datausa.io/profile/geo/pensacola-fl/#demographics.

STRENGTHS and ASSETS:
Military and Public Sector

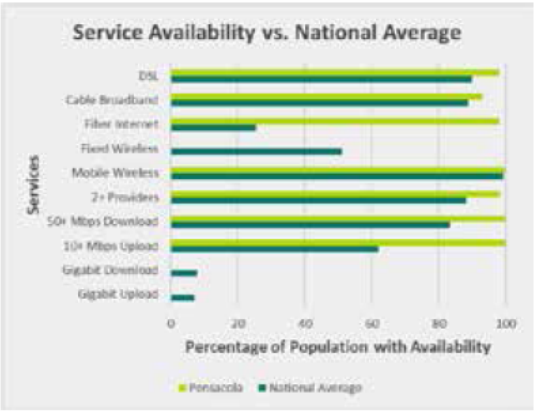
Primary resources exist for developing a strong and visible cyber ecosystem in Northwest Florida. Pensacola offers an appropriate selection of military, commercial, government, academic and training operations necessary for a healthy cybersecurity ecosystem. Many assets, support structures, cyber activities, educational/ training programs, and business development operations currently exist and provide a solid basis on which to grow and expand. While local educational institutions, training programs, and workforce development entities have established the structures to train future cybersecurity professionals, they are in the early stages of development and have yet to generate a significant supply of qualified available workers. With alignment and improved coordination, these programs can greatly impact the Pensacola cyber ecosystem and provide a sustainable cybersecurity workforce. Data portrayed by the CyberSeek organization indicate that a notable cybersecurity workforce exists within the Pensacola area (Fig. 3).

Figure 3. CyberSeek supply and demand Pensacola MSA location quotient. CyberSeek provides data about supply and demand in the cybersecurity job market based on job posting analysis. Source: http://cyberseek.org/heatmap.html

According to CyberSeek, the Pensacola MSA has a high concentration of cybersecurity job demand relative to the national average. CyberSeek indicates that Pensacola's supply/demand ratio of cybersecurity workers is low. With tolerance for variance in the data collected by CyberSeek, the general conclusion can be drawn that cyber workforce supply and demand ratios need improvement. Pensacola should capitalize on local resources including military, education, public and private sectors related to cybersecurity. In particular, defense contractors, aerospace manufacturers, financial and healthcare industries, and information technology/ cybersecurity companies are present in Pensacola.

Military

- Naval Air Station (NAS) Pensacola
- NAS Pensacola Corry Station
- Navy Information Operations Command (NIOC) Pensacola
- Center for Information Warfare Training (CIWT)
- Navy Education and Training Command (NETC)
- Navy Information Warfare Training Command (NIWTC)
- National Security Agency (NSA) National Cryptologic School
- Naval Air Station Whiting Field
- Saufley Field
- Naval Support Activity Panama City
- Eglin Air Force Base
- Air Force Research Labs
- Hurlburt Field (39TH Information Operations Squadron is located at Hurlburt Field)
- Tyndall Air Force Base



Broadband internet in Pensacola, FL. Source: https://geoisp.com/us/FL/pensacola/

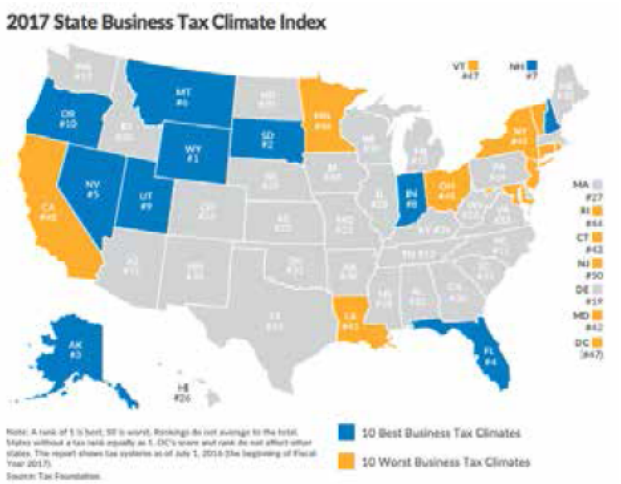
Military (cont.)

- U.S. Fleet Cyber Command
- Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / Industrial Control Systems (ICS) Cyber Emergency Response Team (CERT) and proposed location expansion
- Military personnel and retirees
- World-renowned Blue Angels Flight Demonstration Squadron
- National Naval Aviation Museum
- Barrancas National Cemetery

Infrastructure

- Daily direct flights from Pensacola International Airport to Washington, DC and other locations (Fig. 4).
- Public transportation
- Access to broadband/fiber
- Major CSX East-West Rail Line—runs parallel to Interstate 10, intersected by several short-line railroads that connect to the region's deepwater ports and Norfolk-Southern Rail Lines
- Three Deepwater/Barge Ports—Port Panama City, Port of Pensacola, and the Port of Port St. Joe

Figure 4. Pensacola International Airport .
Source: http://flypensacola.com/page/Air-Service-Development



Business and Living

- No state income tax, low corporate tax rates, and a favorable business tax climate
- Vibrant living and working environment
- World-class healthcare and medical industry

Public Sector Organizations

- FloridaWest Economic Development Alliance
- Achieve Escambia
- Innovation Coast
- AFCEA (Armed Forces Communications and Electronics Association)
- IT Gulf Coast
- Greater Pensacola Chamber
- Enterprise Florida
- Florida Defense Alliance
- Institute for Human and Machine Cognition (IHMC)
- Studer Community Institute

University of West Florida receives designation as a National Center of Academic Excellence in Cyber Defense Education.
Source: UWF Center for Cybersecurity

STRENGTHS and ASSETS:
Private Sector

"Cybersecurity should be a top priority for every business and institution that connects to the Internet. It's exciting that Northwest Florida is quickly becoming a hub for public and private organizations leading the way in defeating online threats. AppRiver is proud to be among those bringing high-quality jobs to a region that already offers an outstanding quality of life."

Michael Murdoch,
President and CEO
AppRiver, LLC

"Pensacola is vitally important in the protection of our nations networks. It is essential that we work together as a community to enhance the workforce pipeline of future cyber talent so that we can continue to grow as a regional leader in cybersecurity. A strong Cyber Strategy will help us accomplish this task and ensure a bright future for the cyber gulf coast".

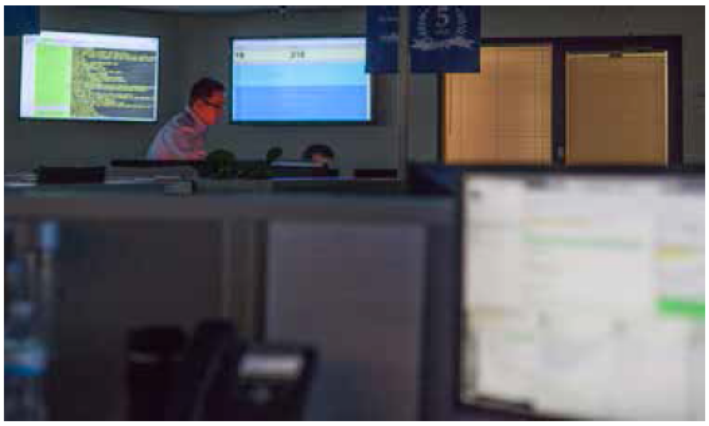
Randy Ramos,
CEO
Global Business Solutions, Inc.

"Greater Pensacola and Escambia County leaders continue to partner toward the enhancement of cyber capabilities as it relates to sense of mission, duty and patriotism in our cyber community."

Keith Wallace Hoskins,
Western District
General Manager
Gulf Power Company

Private Sector

The region is home to more than 500 companies and many industries including advanced manufacturing, information technology, cybersecurity, aerospace and defense, and government contracting. With award-winning IT/cyber companies and corporations located in the Pensacola area, there is much opportunity for growth and innovation.



AppRiver

Private Sector Organizations

- AppRiver, LLC
- Avalex Technologies Corporation
- Baptist Health Care Corporation
- Cognitive Big Data Systems
- Cyber 1 Systems, LLC
- Cyber Safe Workforce, LLC
- CSRA
- EBI Management Group
- Global Business Solutions, Inc. (GBSI)
- Gulf Power Company
- Hixardt Technologies, Inc.
- Metova CyberCENTS
- Navy Federal Credit Union (By 2026, Navy Federal, the largest credit union in the world, is expected to have a $1 billion capital investment in Pensacola, a $425 million payroll and 10,000 employees working on the local campus.)
- Northrop Grumman Corporation
- Raytheon Company
- Sacred Heart Health System, Inc.
- TECHSOFT
- Vor Technology

CyberThon 2016

Cybersecurity Institutions of Higher Education and Training

University of West Florida (UWF)

The UWF Center for Cybersecurity is the regional hub for cybersecurity education and research, outreach activities, and industry partnerships. The university's multidisciplinary approach to cybersecurity education and multiple cybersecurity-related undergraduate and graduate programs has helped the university become a leader in cybersecurity education and workforce development. The university is designated as a National Center of Academic Excellence (CAE) in Cyber Defense Education by NSA and DHS and as the NSA/DHS CAE Regional Resource Center (CRRC) for the Southeast US. These designations are prestigious recognitions for the University of West Florida and surrounding community (Fig. 5).[20]

Figure 5. UWF Cybersecurity Battle Lab.
Source: UWF Center for Cybersecurity

Pensacola State College (PSC)

The Pensacola State College cybersecurity program covers a broad expanse of technological concepts and includes courses in security network technologies and operating systems, security management, and industry best practices. The Bachelor of Applied Science degree in Cybersecurity is built on the eight fundamental domains indentified in the world-renowned (ISC)^2 Certified Information Security System Professional (CISSP) Certification.[21]

Gulf Coast State College (GCSC)

Located in Panama City on Florida's Emerald Coast, Gulf Coast is one of 28 public colleges in the state, all located within commuting distance of 96 percent of the population. GCSC's Network Security Certificate program provides students with a credential for employment in the fast growing cybersecurity field. Students learn how to secure devices, data and networks through an intense, detailed and hands-on training program. GCSC also prepares students to pass industry certifications, including CompTIA Security+ and Cisco CCNA.[22]

George Stone Technical Center (GSTC)

George Stone Technical Center was established in 1968 and partners with local businesses and industries to ensure that training programs prepare students for high demand occupations. GSTC offers an applied cybersecurity program and is a Cisco Networking Academy and Microsoft IT Academy. GSTC helps prepare students for the Microsoft Technology Associate and CompTIA Security+ certification exams.[23]

"Florida's Cyber Coast is home to the NSA/DHS CAE Resource Center for the Southeast US at UWF, nationally recognized cybersecurity education programs and an expanding job market."

Eman El-Sheikh, Ph.D., Director, Center for Cybersecurity University of West Florida

"The cybersecurity program has helped me to greatly expand my skill set," Thibaut said. "Thanks to the training I received, I was able to easily complete the CompTIA Security+ exam. The Battle Lab allows us to gain first-hand experience with different attacks, real-world challenges, and malware mitigation strategies. The program helped me to become a better programmer by demonstrating secure programming practices."

Thomas Thibaut, cybersecurity senior and treasurer of the UWF Cyber Club

STRENGTHS and ASSETS:
Research

"Pensacola is a hidden gem of cyber talent. I had the privilege of working with many local information security professionals who are quietly supporting our nation's critical infrastructure and defense programs."

Michelle Ward, Founder
Cyber Safe Workforce LLC

"Our local Pensacola Blue Angels AFCEA Chapter collaborated with a dynamic cross-section from the Cyber industry, Defense, Intelligence, and Academic partners to create and grow the annual CyberThon event."

Patrick Rooney,
Lead Principal Consultant
Coastal CxO Services, Inc.

Having both worked at Fortune 100 Companies in different parts of the country, including Washington DC, my Business Partner, Mark, and I enjoy the quality of life and work-life balance that Pensacola gives us and our families. There is no better place or better time to be a small business focused on Cyber and Technology than Pensacola in 2017. Small businesses in this community really work together well and know how to team effectively."

Travis Goins,
President
EBI Management Group, Inc.
(VOSB and HUBZone)

Cybersecurity Research Leaders in Florida

University of West Florida (UWF)

The University of West Florida's faculty members and students are engaged in a diverse array of cybersecurity projects including:

- Malware analysis; digital forensics
- Secure software development; security and DevOps
- Artificial intelligence and machine learning for cybersecurity; intelligent cybersecurity education and training tools
- Cybersecurity education and workforce development
- IoT security; security for smart sensor networks
- Cyber physical systems security; critical infrastructure security; aviation security
- Network security
- Human factors and end user error in cyber security
- Risk analysis

Institute for Human and Machine Cognition (IHMC)

The Florida Institute for Human and Machine Cognition (IHMC) is a 501(c)3 not-for-profit organization that pioneers technologies aimed at amplifying and extending human capabilities. IHMC is at the forefront of cybersecurity with many areas of interdisciplinary research including designing large scale interactive network event visualizations, understanding cyber deception tactics, applying moving target defenses, developing intelligent software agents, and automating security policy reasoning and enforcement.[24]

UWF Cybersecurity Battle Lab.
Source: UWF Center for Cybersecurity

Studer Community Institute

The Studer Community Institute is focused on improving the community's quality of life. The cornerstone of the Institute's work is the Pensacola Metro Dashboard. The dashboard consists of 16 metrics, developed with the University of West Florida, to provide a snapshot of the educational, economic and social well-being of the community. The dashboard permits the comparison of the community's performance to other similarly sized communities in measures ranging from high-school graduation rates to household incomes.[25]

OPPORTUNITIES

The military presence has enabled Pensacola to establish a foundation for cyber growth, and the region is poised to be a leader in the cybersecurity industry. Military missions fuel contract opportunities in the area. Naval Air Station Pensacola has space to grow and its growth would increase contract opportunities for businesses in close proximity to the military facility. Retaining a military presence is important for cybersecurity business expansion, government contracts, and entrepreneurial ventures.

While military and government contract work is critical, economic and resource diversification reduces risk and creates long-term sustainability. A balanced portfolio of industries pursuing cybersecurity growth (e.g., financial, manufacturing, healthcare, and technology) is needed for Pensacola's cyber success. Leveraging resources for existing IT/cyber businesses and new businesses entering the cybersecurity industry will support diversification.

An emerging opportunity for Pensacola is industrial control systems (ICS) cybersecurity. In 2015, the NCCIC expanded operations in Pensacola. "ICS-CERT reassigned its production chief from Arlington, Virginia, to Pensacola and the senior watch officer began watch operations in Pensacola."[26] A feasibility study is needed to determine market potential for ICS commercial sectors that should be targeted.

Pensacola has the opportunity to compete and partner with other established cyber hubs. Pensacola is ready to build momentum, fulfill the vision of "Live Coastal. Work Cyber.," and create a cyber culture. Success requires stakeholders to adopt a unified strategy that will make Pensacola's Cyber Coast the choice place to live and perform cyber work. The combined strengths of Pensacola, FL, Atlanta/Augusta, GA, and Huntsville, AL, collectively comprise a southeastern cybersecurity region. With unified efforts, this southeastern megahub could emerge as a leader for the nation in cybersecurity.

GOALS and STRATEGIES MATRIX*

	Priority	Timeframe		Implementation Stakeholders
		Short-Term 6-12 mo.	Long-Term 5+ yrs	
Goal 1: Build a thriving cybersecurity workforce				
1.1 Create cyber career pathways to employment		X		
1.2 Integrate cyber education into public school curricula			X	
1.3 Align post-secondary higher education entities to meet industry needs			X	
1.4 Recruit and retain a diversified workforce		X		
1.5 Military personnel transition		X		
1.6 Develop mentorship and/or apprenticeship programs		X		
1.7 Create an adaptive learning workforce			X	
Goal 2: Strengthen partnerships to enhance cybersecurity innovation and economic development				
2.1 Create cybersecurity council of key stakeholders		X		
2.2 Develop regional strategy for cybersecurity economic growth		X		
2.3 Develop information sharing frameworks		X		
2.4 Leverage local cybersecurity contacts		X		
2.5 Provide local cyber entrepreneurship/innovation development and support		X		
Goal 3: Enhance technology infrastructure and optimize cybersecurity business climate				
3.1 Determine need for increased broadband/fiber access		X		
3.2 Increase public and private sector technology enabled services			X	
3.3 Establish a shared cyber innovation range or center of excellence		X		
3.4 Host major cyber conferences and events			X	
3.5 Offer cybersecurity focused business incentives			X	
3.6 Create a central point of contact for cyber		X		
3.7 Retain and increase federal missions		X		
Goal 4: Market the Pensacola region's "Live Coastal. Work Cyber." brand				
4.1 Create an aggressive marketing plan for the region		X		
4.2 Choose the optimal marketing tools		X		
4.3 Promote "Live Coastal. Work Cyber."			X	

*Note: The matrix provided above is the guiding framework to enable the community to establish priorities and implement strategies for cybersecurity industry growth.

References:

1. https://niccs.us-cert.gov/glossary#C
2. https://www.doleta.gov/usworkforce/whatsnew/eta_default.cfm?id=6795
3. http://technet.org/state-policy/smart-infrastructure
4. http://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_51510.pdf
5. http://www.crda.org/news/local_news/spawar-atlantic-breaks-ground-on-new-building/
6. https://fcw.com/Articles/2007/02/12/DISA-to-pay-12B-for-network-protection.aspx
7. http://www.disa.mil/About/Our-History/2000s#jtf
8. http://www.disa.mil/About/Our-History/1990s
9. http://tools.netsa.cert.org/silk/index.html
10. https://fcw.com/articles/2007/02/12/disa-to-pay-12b-for-network-protection.aspx
11. https:// www.dhs.gov/creation-department-homeland-security
12. http://archive.defense.gov/news/newsarticle.aspx?id=60755
13. https://archive.is/20120719215756
14. http://www.af.mil/news/story.asp?id=123221046
15. https://www.dhs.gov/einstein
16. https://www.defense.gov/News/Article/Article/603083
17. http://www.disa.mil/Cybersecurity/Analytics/Acropolis
18. https:// fcw.com/articles/2013/08/12/disa-nsa-cloud-model.aspx
19. http://www.stratcom.mil/Media/ Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom
20. http://uwf.edu/go/cybersecurity
21. http://www.pensacolastate.edu/academic-programs/cybersecurity
22. https://www.gulfcoast.edu/academics/programs/network-security-cybersecurity-certificate/index.html
23. http://www.georgestonecenter.com
24. http://www.ihmc.us
25. http://studeri.org/dashboard
26. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

Acknowledgements

To FloridaWest Economic Development Alliance, the University of West Florida Center for Cybersecurity, members of the Cybersecurity Advisory Group (Appendix H), and all of the public and private stakeholders committed to making our region a leader in cybersecurity, I would like to express heartfelt appreciation for graciously contributing time, knowledge, experience, and insights. I would like to recognize Dr. Eman El-Sheikh, Director of the University of West Florida Center for Cybersecurity, for generously sharing her time and expertise. I offer my sincere gratitude to the industry experts and professionals that participated in the interview process, provided information, attended the cybersecurity strategic planning workshop, and contributed to the planning and development process. Special thanks to: Lori Anderson, Danita Andrews, Rob Bichan, Dr. Kirk Bradley, Rick Byars, Paul Carney, Bob David, Bill Dunn, Christopher Eng, Travis Goins, Guy Garrett, Jennifer Grove, Neil Gaudreau, Dr. Brice Harris, Keith Hoskins, Harry Huelsbeck, Zach Jenkins, William Knehr, Kristie Kelley, Manfred Laner, Paul Lashmet, William Lintz, Kristin Longley, Scott Luth, Sena Maddison, Matt Matzer, Andrea Moore, Beth McClean, Jim McClellan, Christopher Middleton, Dustin Mink, Ray Murphy, David Musselwhite, Dr. Pamela Northrup, Peter Nowak, Sean O'Brien, Shannon Ogletree, Anthony Pinto, Robert Pratten, Don Quinn, Randy Ramos, Kelly Reeser, Lloyd Reshard, Andrew Roach, Patrick Rooney, Dr. Martha Saunders, Mike Shanholtz, Mel Stinson, Lee Stubbs, Dr. Michelle Taylor, Gregory Touhill, Jonathan Tucker, Greg Voss, Julia White, Tim White, and Michelle Ward.

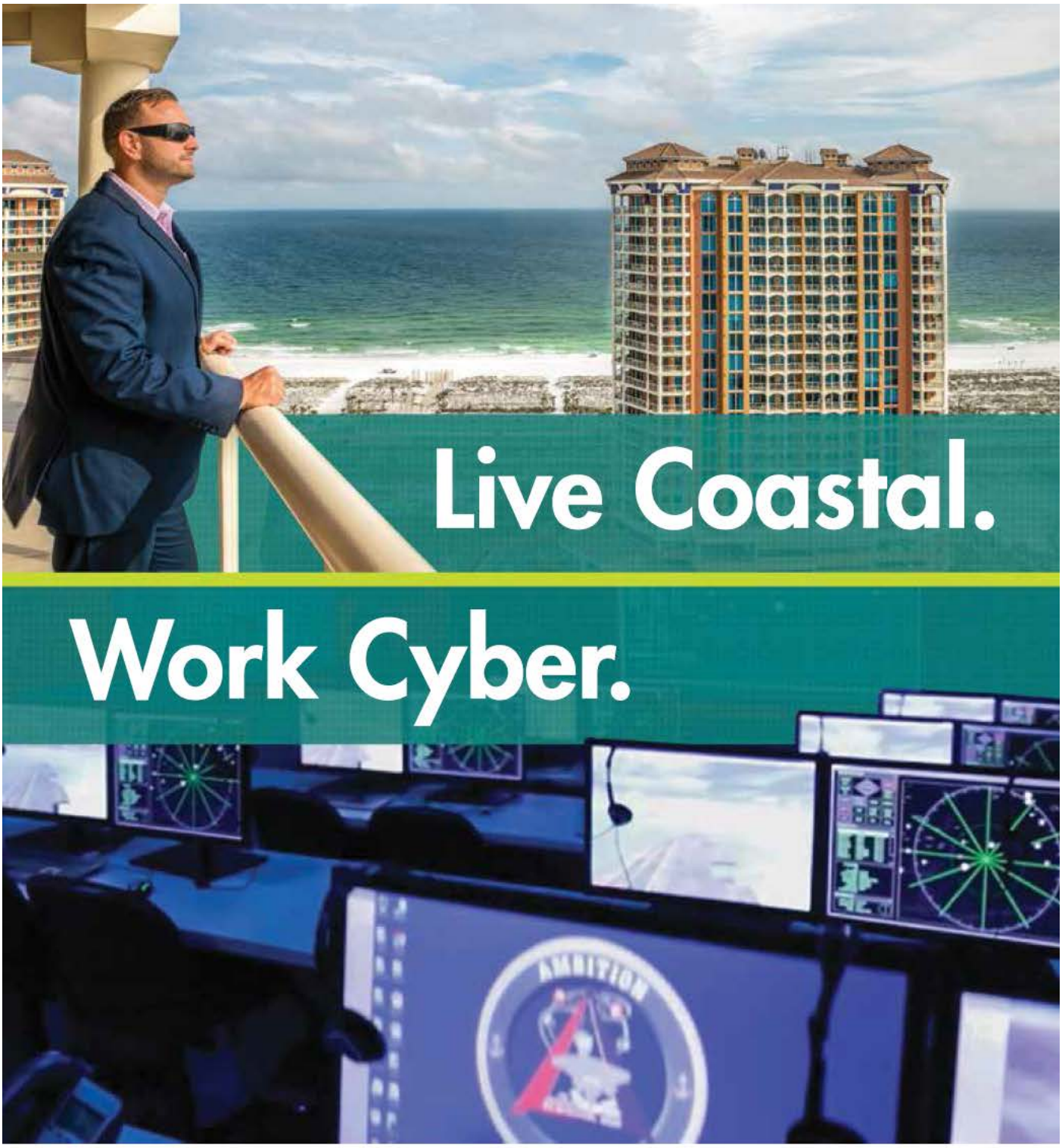
Janet Woolman
Innovation Strategies, LLC

Janet Woolman received her Master of Library and Information Science degree from Louisiana State University in Baton Rouge, Louisiana. Ms. Woolman is the owner of Innovation Strategies, LLC, located in Gulf Breeze, Florida. Ms. Woolman also is a Visiting Lecturer for Economic Development and Innovation at McNeese State University in Lake Charles, Louisiana, and is a Planning Consultant with FloridaWest in Pensacola, Florida.

Jeanne Daboval received her Doctor of Business Administration in Human Resource Management degree from Nova Southeastern University in Fort Lauderdale, Florida. Dr. Daboval served as Provost and Vice-President for Academic Affairs at McNeese State University in Lake Charles, Louisiana, for over 15 years.

William Dees received his Doctor of Philosophy in Ecological Sciences degree from Old Dominion University in Norfolk, Virginia. Dr. Dees is a retired naval officer. Currently, Dr. Dees is a Professor of Biological Science at McNeese State University in Lake Charles, Louisiana.

Lyle Hardee received his Master of Science in Mathematical Sciences with a Concentration in Computer Science degree from McNeese State University in Lake Charles, Louisiana. Mr. Hardee is an Instructor of Mathematical Sciences at McNeese State University in Lake Charles, Louisiana.



To find out how contact:

FloridaWest

850.898.2201

FloridaWest™

economic development alliance