FISSEA 34th Annual Conference: Refining Cybersecurity Culture: WIIFM*

May 14-15, 2024
Rockville, MD

*What’s in it for me?
Federal Information Security Educators (FISSEA)

34th Annual FISSEA Conference

“Refining Cybersecurity Culture: WIIFM”

May 15, 2024
9:00am – 3:00pm ET
Please Note...

This webinar and the engagement tools will be recorded.

An archive will be available on the event website.
Conference Welcome

Brooke Crisp
FISSEA Co-Chair

Frauke Steinmeier
FISSEA Co-Chair

#FISSEA | nist.gov/fissea
Get Involved

Subscribe to the FISSEA Mailing List
FISSEAUpdates@list.nist.gov

Volunteer for the Planning Committee
https://www.nist.gov/itl/applied-cybersecurity/fissea/meet-fissea-planning-committee

Serve on the Contest or Award Committees for 2025
Email fissea@list.nist.gov

Submit a presentation proposal for a future FISSEA Conference or FISSEA Forum
https://www.surveymonkey.com/r/fisseacallforpresentations
PANEL
CISA’s Federal Cyber Defense Skilling Academy

Marian Merritt
Deputy Director of NICE
National Institute of Standards and Technology

Sharon McPherson
Senior Cybersecurity Specialist for
Policy Training & Awareness
Department of Veterans Affairs

Maureen Premo
Cyber Defense Education and Training (CDET)
Cybersecurity and Infrastructure Security Agency

#FISSEA | nist.gov/fissea
FEDERAL RESKILLING AND UPSKILLING PANEL

Sharon F. McPherson
Sr Cybersecurity Specialist for Policy, Training & Awareness

Office of Information and Technology

FISSEA  May 2024

FOR INTERNAL USE ONLY
Career Development Portal (CDP) - Technical Track
Career Development Portal - TSS Work Role
### Covered During Period?

<table>
<thead>
<tr>
<th>Task</th>
<th>Proficiency Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>T0237:</strong> Troubleshoot system hardware and software.</td>
<td></td>
</tr>
<tr>
<td>1. Gather information about how to troubleshoot system hardware and software.</td>
<td></td>
</tr>
<tr>
<td>2. Understand what tools are available [i.e., DBAT, Vault] and when to use them to troubleshoot system hardware and software.</td>
<td></td>
</tr>
<tr>
<td>3. Utilize various MS Teams or other established platforms to find information and ask questions.</td>
<td></td>
</tr>
<tr>
<td><strong>T0468:</strong> Diagnose and resolve customer reported system incidents, problems, and events.</td>
<td></td>
</tr>
<tr>
<td>1. Gather information about how to resolve basic customer reported issues, including system incidents and events.</td>
<td></td>
</tr>
<tr>
<td>2. Communicate with customers to gather basic information necessary to assess the reported issue.</td>
<td></td>
</tr>
<tr>
<td>3. Research possible solutions using multiple methods [e.g., Knowledge Base, Google, etc.].</td>
<td></td>
</tr>
<tr>
<td>4. Consult with more experienced IT specialists after attempting all known possibilities to resolve the issue.</td>
<td></td>
</tr>
<tr>
<td><strong>T0491:</strong> Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.</td>
<td></td>
</tr>
<tr>
<td>1. Shadow experienced peers for hands-on learning of installation and configuration of hardware, software, and peripheral equipment and troubleshooting.</td>
<td></td>
</tr>
<tr>
<td>2. Independently install and configure hardware, software, and peripheral equipment within organizational standards.</td>
<td></td>
</tr>
</tbody>
</table>
VA Cybersecurity Apprenticeship Program for Veterans (VA CAPV)
VA CAPV Program Cycle – Mentoring Details

Skills Maturity Assessments

Formal Training Courses

On-the-Job Training

Mentoring

Senior Mentor

Experienced Mentor

Cohort Mentoring
VA CAPV Program Cycle – On-the-Job Details

Skills Maturity Assessments  Mentoring

Formal Training Courses  On-the-Job Training

Job Shadowing  Hands-on Learning  Skill Execution

FOR INTERNAL USE ONLY • OFFICE OF INFORMATION AND TECHNOLOGY
VA CAPV Program Cycle – Formal Training Details

Skills Maturity Assessments

Mentoring

In-Person Instructor-Led Trainings

Online Live Trainings

Online Self-Paced Trainings

Certificate Programs
VA CAPV Program Cycle – SMA Details

Skills Maturity Assessments

Demonstration of Knowledge

Required Supervision or Oversight

Complexity to Perform Work
CISA’S FEDERAL CYBER DEFENSE SKILLING ACADEMY

FISSEA
May 2024
Maureen Premo
maureen.premo@cisa.dhs.gov
Cybersecurity Workforce Landscape

The Federal Cyber Defense Skilling Academy (FCDSA) was created in response to the 2019 Presidential Executive Order 13870: America’s Cybersecurity Workforce and aims to make a positive impact by mitigating existing cyber workforce gaps. As of October 2023, the following data spotlights both challenges and opportunities in the current cyber workforce landscape.

- **92%** of cybersecurity staff report having skills gaps in their organization.
- **82%** increase in federal cybersecurity job openings since 2010.
- **572,392** Total National Cybersecurity Job Openings.
- **68%** growth is needed to meet current global demand.


Cyberseek.org (12 Dec 2023)
In FY22, the Skilling Academy launched its inaugural course, offering students an opportunity to focus on professional growth through an intense, full-time, three-month accelerated cyber training program open to federal employees.

All courses are developed in alignment to the knowledge, skills, and abilities (KSAs) required for their respective cyber work roles as defined in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

**Skilling Academy Program features:**
- Instructor-led 12-week course, 40-hour/week commitment, taught 100% virtually.
- Training consists of a mix of lectures, practices in realistic lab environments, and assessments.
- Students receive training which is aligned to globally recognized certifications.

**Current Offerings**
- Cyber Defense Analyst Pathway
- Cyber Defense Forensics Analyst Pathway
- Cyber Defense Incident Responder Pathway
- Vulnerability Assessment Analyst Pathway
FY24 Skilling Academy Course Offering Expansion

In FY24, the Skilling Academy is offering three new courses mirroring the existing framework of the inaugural Cyber Defense Analyst (CDA) Pathway.

- **Duration**: 12-Weeks
- **Number of Participants**: 20-25 Students per Pathway
- **Target Audience**: Full-time Federal Employees

**Cyber Defense Forensics Analyst Pathway**
- **Goal**: Develop the skills required to investigate and analyze digital evidence in support of vulnerability mitigation.
- **Eligible Certification**: EC Council’s Computer Hacking Forensic Investigator (CHFI)

**Cyber Defense Incident Responder Pathway**
- **Goal**: Develop the skills required to accurately identify, assess, and mitigate security incidents within a digital environment.
- **Eligible Certification**: CompTIA’s Cybersecurity Analyst (CySA+)

**Vulnerability Assessment Analyst Pathway**
- **Goal**: Develop skills required to engage in penetration testing and vulnerability management to prevent cyberattacks.
- **Eligible Certification**: CompTIA’s Penetration Testing (PenTest+)
For more Information: Federal Skilling Academy

Questions?
SkillingAcademy@cisa.dhs.gov
Artificial Intelligence and Cybersecurity

Harold Booth
National Institute of Standards and Technology
Artificial Intelligence and Cybersecurity

Harold Booth
National Institute of Standards and Technology
Artificial Intelligence and Cybersecurity
Agenda

• Definitions
• Trustworthy Artificial Intelligence
• AI Risk Management
• NIST Work
Definitions

Executive Order 14110: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

The term “artificial intelligence” or “AI” has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.
Additional Terms

Machine Learning
Generative AI
Foundation Models
Frontier Models
AI Red-Teaming
AI Opportunities

- Translation
- Speech Recognition
- Automate Repetitive Tasks
- Find Patterns
- Aid Human Decision Making
Core Building Blocks of Trustworthy AI

- Safe
- Secure & Resilient
- Explainable & Interpretable
- Privacy-Enhanced
- Fair - With Harmful Bias Managed
- Accountable & Transparent

Valid & Reliable
Some Cybersecurity Questions to Ask:

- What is the task?
- Is AI necessary?
- What are the threat & deployment assumptions?
- Which attacks are still relevant?
- What metrics are applicable to highest priority risks?
- What experiments can generate those metrics?
AI Risks

Consumer
- Intellectual Property
- Unreliable Output

Producer
- Data Protection
- Protect ML Tool Chain
- Input Validation

Landscape
- Synthetic Content
- New Fraud Uses
- Heterogeneity

Document/Image Generation, Classification
Chatbots, Classifier
Identity Verification, Email, Information Ecosystem
Adversarial Machine Learning
Adversarial Machine Learning
Summary

Understand Task

Evaluate Risks

Implement and Deploy

Monitor and Manage Incidents
The President’s Executive Order (E.O.) on Safe, Secure, and Trustworthy Artificial Intelligence (14110) directs NIST to:

### Create Guidance
- Generative AI and dual-use foundation models
- Differential-privacy guarantee protections
- Red-teaming/testing
- Authenticity and provenance of synthetic content

### Develop Evaluation & Testing
- Test environments for evaluating AI capabilities, including those that could cause harm
- Availability of testbeds supporting the development of safe, secure, and trustworthy AI technologies

### Engage with Stakeholders & Develop Standards
- Global engagement on AI standards
- Synthetic nucleic acid synthesis providers engagement
- Minimum risk-management practices
NIST’s Progress on E.O.

- Request for Information to inform NIST’s assignments
- Draft Guidelines for Evaluating Differential Privacy
- Secure Software Development Framework Workshop
- Pre-release testing of NIST’s Dioptra infrastructure
- Synthetic Content Report under interagency review
AISI Consortium

November 2023: Release of Federal Register Notice (FRN) asking for letters of interest—over 600 received!

February 2024: Official launch of Consortium with inaugural cohort of more than 200 member companies

February 2024: Begin working with partners across five working groups

March 2024: Set work plans for the five working groups

Credit: NIST
AISI Consortium Working Groups

Risk Management for Generative AI

Synthetic Content

Capability Evaluations

AI Red-Teaming

Safety & Security
Flexible and Modular Evaluation

- **Model Architecture**
  - Shallow Net
  - AlexNet
  - LeNet
  - ResNet50
  - VGG16
  - ...

- **Data Augmentation**
  - Patch augmentation
  - Poison Frogs
  - Adversarial training
  - ...

- **Inference preprocessing**
  - Spatial smoothing
  - Defensive distillation
  - ...

- **Dataset**
  - MNIST
  - Fruits360
  - ImageNet
  - ...

- **Attack on trained model**
  - Fast Gradient Method
  - Pixel Threshold
  - Patch
  - Membership Inference
  - ...

- **Metric**
  - Clean accuracy
  - Adversarial accuracy
  - Robustness radius
  - ...

Web: https://github.com/usnistgov/dioptra
Email: dioptra@nist.gov
Questions?
Contact


https://airc.nist.gov/


AIFramework@nist.gov
usaisi@nist.gov
References

- Executive Order 14110: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
- NIST AI 100-1: Artificial Intelligence Risk Management Framework (AI RMF 1.0)
- OWASP Top 10 for Large Language Model Applications
References

- Deploying AI Systems Securely
- Guidelines for secure AI system development
- Engaging with Artificial Intelligence
Backup
Two Attacks, Three Defenses

FGM Attack:

- Patch Attack:

Defenses:
- Spatial Smoothing
- Gaussian Augmentation
- JPEG Compression
Attack and Mitigation Interfaces in the Model Lifecycle

- Poisoning
- Evasion
- Oracle

Sample of attack interfaces

Sample of mitigation interfaces
CyberSecureFlorida: A Cyber-Readiness Blueprint for the Nation

15 MAY 2024
WHO ARE WE?

Established in 2014: FS 1004.444
Housed at USF to make Florida “the national leader in cybersecurity”

Education
Build and expand Florida's cybersecurity educational cybersecurity workforce development

Research
Enable and expand cybersecurity research capabilities across the state and enable technology innovation, transfer, and adoption

Community Outreach and Engagement
Enable community engagement and collaboration to raise cyber-awareness and resilience across the state

Cybersecurity Public Policy
Guide and shape public policy to enhance cybersecurity across the state.
WHAT ARE WE DOING?

Making Florida the national leader in cybersecurity (FS 1004.444)

GRANT-FUNDED & STATE INITIATIVES

Florida’s Cybersecurity Critical Infrastructure Risk Assessment
Conduct a voluntary cybersecurity risk assessment for Florida-based public and private critical infrastructure organizations

Statewide Cybersecurity Training Program
Provide cybersecurity awareness and training courses tailored to job roles for all public-sector employees

Cyber Range (HB 5001)
Provide a cost-effective, realistic cybersecurity training environment for city, county, and local governments

CyberWorks: Cybersecurity Workforce Development (NCAE)
Prepare veterans and transitioning first responders for jobs in cybersecurity
WHAT ARE WE DOING?

Making Florida the national leader in cybersecurity (FS 1004.444)

ONGOING PROGRAMS

Operation K12
Infuse cybersecurity awareness and career preparation throughout the Florida education system

CyberLaunch NEW!
Florida’s first statewide high school cyber competition

Teaching Digital Natives (TDN)

Outreach & Events
Educate through public awareness campaigns and host events to help vulnerable organizations enhance their cyber posture; Sunshine Cyber Conference

Policy & Research
Fund and facilitate research and help guide public policy by educating both the decision-makers and the public on best practices and policy initiatives

SOCAP: Security Operations Center Apprentice Program
Provide hands-on experience to complement degree programs and services to support the public sector
FLORIDA STATEWIDE CYBERSECURITY TRAINING

• HB5001, Section 2944B
• $30M non-recurring
• In consultation with the Department of Management Services and the Florida Digital Service
• In consultation with the Florida Cybersecurity Advisory Council

Education AND Training

Our aim is to have the State of Florida set the example in cybersecurity awareness, preparedness that meets NIST standards.

Critical Infrastructure Risk Assessment (CIRA) CSET results from INL: Leaders need to know more about cybersecurity and organizations need to elevate their standards to the NIST standards.

University of South Florida (USF):
• Cybersecurity Awareness Certificate for FL SLTT Employees
  • The Florida Digital Service (FLDS) Local Resource Packet
• Cybersecurity Mgmt Training for FL SLTT Mid-Level Managers
• GIAC GSLC industry certification prep course and exam (coming soon)

University of West Florida (UWF):
• CompTIA and ISC2 industry certification prep courses and exams
• Technical Courses: AI and Machine Learning, Threat Intelligence
• Cyber Skills Exercises : Policy Writing, Ransomware, Phishing Scenarios
Florida International University (FIU):
- Executive Seminar in Cybersecurity Leadership & Strategy
- Onsite Leadership training and seminars (catered to org. needs)
- FIU partners with 7 institutions across the state to minimize travel while providing more in-person sessions
- Online executive training course (coming soon)

National White Collar Crime Center (NW3C):
- 3-day, in-person classes for FDLE focusing on cybercrime investigation
  - Dark Web, Crypto Currency

Norwich University Applied Research Institute (NUARI):
- Partner hosted Election Security Tabletop Exercises in-person 70 participants. CISA, FBI, FDLE, SimSpace, FLDS, County Sheriffs, SOE.
CyberSecureFlorida Training programs continues to make an impact reaching 96% of Florida’s counties (64 out of 67).

The CyberSecureFlorida program now has over 40 courses and Tabletop Exercises available, including industry certifications prep courses with exam fees at no-cost.

“This program is unique in having an entire class who are all experiencing the same things as you. It is much easier to have discussions when everyone is on the same page and it’s not local government in the same class as the private sector with unlimited resources. It also allows you to expand your network and interact with others so that you can exchange ideas and discuss problems after the class is over.”

- Heather Stevenson, IT Manager, Clay County Sheriff’s Office
Lessons Learned:

• No-Cost may also mean no investment by participants. “Whats in it for me?”
• Endorsements play a critical role in validation and social proof that can influence decisions in the community.
  Leadership support / Endorsements have weight.
• The market is competitive with many players who have more public notoriety, thus unique value propositions are needed to remain relevant.
• Collaboration with state agencies is crucial to building a complementary program. New mandates mean new training curriculum.
• Listen to your partners.
• Build relationships.
• Promote – Execute – Follow Up – Promote More.
• Be creative in problem solving (there is always a solution).
  IAFCI Cyber Fraud Summit, Cyber Florida ARCS Range and more.
ESTABLISH A TRAINING CYBER RANGE (HB5001)

- $10M non-recurring
- $500K recurring

RANGE FEATURES

- Florida County and Local government IT and cybersecurity personnel - public sector focused
- Cyber Range as a Service (CRaaS), 100% cloud-based training model
- No cost for public sector users
- Support Statewide Training Program

KEY MILESTONES

✓ SimSpace chosen as vendor in Feb 2024; soft launch in Feb 2024 - "Aligned Realistic Cyberattack Simulation (ARCS)" Range
✓ Ribbon cutting of formal launch on 27 March 2024
✓ Currently 116 users across 13 counties on ARCS Range
• Coalition member of the National CAE Cybersecurity Workforce Development Program: CyberSkills2Work
• $1.5M NSA/DHS Grant
  • Renewed in June 2023
• Industry partners include JPMorgan Chase, ReliaQuest, KnowBe4, Amazon Web Services, VMWare, Rapid7, Cisco, Raytheon, OPSWAT, GuidePoint

CYBER DEFENSE ANALYST PATHWAY

• **NICE Work Role:** Cyber Defence Analyst
• **Number of Learners:** 109 completed over two years.
• **Courses/Badges:** Network Fundamentals, Cyber Defense Fundamentals
• **Industry Certifications:** CompTIA Network+ and CompTIA Cybersecurity Analyst (CySA+)

Supports statewide training program and Cyber/IT Pathways Grant Project
RECENTLY COMPLETED 14-MONTH PROGRAM TO EXPAND FLORIDA’S CYBER EDUCATION INFRASTRUCTURE

- $21M project to boost cybersecurity education statewide through subawards to public education institutions
- Facilitated 31 Subawards to State Universities, State Colleges, and School Districts
  - Scholarships at all levels
  - Recruiting for cybersecurity degree programs
  - Internships and Apprenticeships
  - Industry certifications
  - New and revised course content
  - Adult workforce development
  - Summer camps, training sessions, competitions, conferences
- Project period: 2022-2023

Producing playbooks so schools nationwide can implement these programs
SUMMARY

CYBER FLORIDA IS FULLY ENGAGED
- Risk Assessment
- Education and Training
- Cyber Range
- Workforce Development

A STATEWIDE RESOURCE
- Engaged across the State
- Public and Private Sector

HELPING TO MAKE FLORIDA THE LEADING STATE IN CYBERSECURITY
Cybersecurity Workforce Renaissance

Allen Westley
Director Cybersecurity
Space and Airborne Systems
Welcome, colleagues. Today, we embark on a journey to bridge the workforce gap in cybersecurity.

by Allen Westley
The Current Workforce Landscape

1. Challenges Ahead
   An honest look at the cybersecurity workforce void and its implications across industries and global security.

2. Ripple Effect
   The reciprocating consequences of these vacancies resonate far and wide, impacting privacy and economic fabric.
Bridging the Workforce Divide: Industry's Role

Educational Syllabi Integration
Championing authentic cybersecurity challenges in academic programs to prepare a resilient workforce.

Mentorship Triumphs
Illuminating tales of successful mentorship propelling individuals to new career heights.

Inclusivity and Empowerment
A call for embracing diverse recruitment and leadership models in our collective pursuit.
Innovative Talent Cultivation Approaches

1. AI in Talent Scouting
   Exploring AI and machine learning’s role in identifying cybersecurity talents worldwide.

2. Adaptability in Training
   Emphasizing the need for flexible and forward-looking training strategies in cybersecurity education.

3. Creating Ingress Pathways
   Outlining the role of internships and alternative educational frameworks in expanding our talent reservoir.
Unity for Cybersecurity Workforce

1. Fostering Partnerships
   Encouraging collaboration and shared ventures to address the cybersecurity workforce gap.

2. Anticipatory Leadership
   Inspiring forward-thinking leadership strategies to proactively tackle emerging challenges.

3. Personal Growth Focus
   Promoting a culture of continuous learning and personal development within the cybersecurity domain.
Thought Leadership: Looking Towards the Future

 Strategic Collaborations
 Exemplifying cross-sector partnerships as a keystone for addressing the workforce gap.

 Resilience and Integrity
 The ethos of leading by example with unassailable integrity and resilience in the face of challenges.

 Career Mastery Ethos
 Urging professionals to embrace a trajectory of mastery and unending learning in their careers.
Personal and Professional Growth

Collaboration
Fostering a culture of collaboration, knowledge sharing, and collective problem-solving in the cybersecurity community.

Vision
Instilling a visionary outlook to anticipate and address future cybersecurity workforce challenges proactively.

Growth Mindset
Promoting a growth mindset to foster continuous learning and career development in cybersecurity roles.
Cybersecurity Future: A Unified Vision

<table>
<thead>
<tr>
<th>Cybersecurity Collaboration</th>
<th>Cybersecurity Visionaries</th>
<th>Growth Mindset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global partnerships to bridge workforce gaps</td>
<td>Industry leaders foreseeing future challenges</td>
<td>Continuous learning and career development ethos</td>
</tr>
</tbody>
</table>
Cyber Renaissance Conclusion

Visual Representation
A futuristic cityscape infused with digital security symbols, exuding an aura of technological innovation and energy.

Synergistic Unity
A united team of cybersecurity professionals, exuding forward-thinking dynamism and collaborative synergy.

Cyber Renaissance
Iconic representation of innovative cybersecurity advancements, future-proof technologies, and diverse talent shaping the cyber renaissance.
Security Awareness Reimagined

Mindy Baird
Senior Information Security Risk Specialist
Western & Southern Financial Group
Security Awareness Reimagined

Mindy Baird
Western & Southern Financial Group
Mindy Baird, CISA, CRISC, CIPP, CTPRA, CDPSE, SSAP

Senior Information Security Risk Specialist

4 years with Western and Southern Financial Group
  Security Awareness Program Owner
  Third-party Risk Management Assessor

31 years with Procter and Gamble
  Information Security, Internal Audit, Global Data Privacy manager

Infragard – Cincinnati Chapter
FBI Citizens Academy Alumni
Security Awareness Reimagined

THE SAME OLD THINKING

THE SAME OLD RESULTS

A
The world we have created is a product of our thinking; it cannot be changed without changing our thinking.

(Albert Einstein)
Definition of Reimagine

• To imagine or conceive something in a new way.

Opposite of Reimagine

• Crush, damage, demolish, destroy, harm, ignore, impair, prevent, remain, stay, wreck
Agenda

• Reimagine how you manage risk
• What’s working/not working
• Why
• Relationships
• Engagement on a budget
• Metrics
• How to remain resilient
Status Quo

- We must change our approach to security awareness if we wish to see employee behavior change.
Risk Management through Behavior Change

Compliance vs. psychology/human behavior

- Goal/Objective
- What’s Working/Not Working
- Reaching employees
- Measuring Success

Risk Management
Changing Behavior

Our ultimate objective is to manage risk by changing employee behavior.

- Will our current image do that?
- How do we change it?
- Take time to explain
- Don’t just tell them to do something.
Relatable

- Different Knowledgebase
- Informing/Educating
  - What data do they handle?
- What makes them care?
  - Make it personal
B.J. Fogg Behavior Model

Behaviormodel.org
Relationships

- The Business
- Focus Groups
- Security Champions
- Advisory Board
Understanding the Business
Focus Groups

- A day in the life
- Goals/hurdles
- Their view of Security
- Become their partner
- Same team/shared objectives
Security Champions

Advisory Board
Engagement on a Budget

Security compliance can generally address known threats but it takes a fully engaged workforce to deal with new and unknown attack vectors.

- Approachable
- Make it fun
- Think outside the box
- Reward and Incentivize
Approachable

- How are you being approachable?
Make it Fun

• Their interests
• Motivators
• Doesn’t have to be big
• Be creative
Think Outside the Box

• What are others in your industry doing?
  – Ask “Around” Table

5 Senses  Videos  Panel  FAQs  Speakers  Comms – Banners, News section
Videos
Reward and Incentivize

- Positive reinforcement
- No budget? No problem
- Security Nominations

Never underestimate the power of stickers.

Rewards Just Ahead
Keep Security in Forefront all Year
Plan Your Activities

Change your image

JUNE 2011

Sunday Monday Tuesday Wednesday Thursday Friday Saturday
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30

Western & Southern Financial Group

Security

 PROPRIETARY
Metrics

• Baseline
• Positive results – who reported vs who clicked.
• Dashboard
• Audience
• Revisit regularly, at least annually.
Remaining Resilient

- Covid
- Budget cuts
- Employee turnover
- Increased phishing
- Ransomware on the rise

- *Principles and Objectives

**Resilience**

/rɪˈzɪlɪəns/
in noun

1. the ability of a substance or object to spring back into shape; elasticity.
   "nylon is excellent in wearability and resilience"

2. the capacity to recover quickly from difficulties; toughness.
   "the often remarkable resilience of so many British institutions"
Remaining Resilient

- Reduce risk through behavior change
- Ensuring engagement
- Risk will continue to change, and how we tackle that remains fluid.
  - Ransomware Readiness
  - AI

- Develop a program that allows you to exchange Risk A for Risk B, and allow you to flow to the risk in a way that reflects your principles and objectives.
Recap

- Reimagine/Think outside the box
- Compliance through engagement
- Relationships
- Shared Understanding
- Shared Objectives
- “Way of life” – year-round vigilence
- Metrics

Just because they are aware, doesn’t mean they care.
Challenge the Status Quo

Learn from yesterday, live for today, hope for tomorrow. The important thing is not to stop questioning.

(Albert Einstein)

Western & Southern Financial Group
Questions?

Contact me: 
Mindy.baird@westernsouthernlife.com
34th Annual FISSEA Conference

Lunch and Exhibitor Showcase

12:15pm-1:00pm ET

#FISSEA | nist.gov/fissea
Welcome Back!

Brooke Crisp
FISSEA Co-Chair
Empower, Equip, Defend: Building a Cyber-Ready Federal Workforce

Nat Prakongpan
VP of Product
Cyberbit

#FISSEA | nist.gov/fissea
Empower, Equip, Defend
Building a Cyber-Ready Federal Workforce
AGENDA

01 Federal Government Cybersecurity
   The Critical Need for a Skilled Workforce

02 Engaging Learners, Retaining Knowledge
   Challenges of Traditional Training Methods

03 Learning Methods that Empower the Workforce
   Incentive-Based, Hands-On Approaches, Crisis Simulations

04 Live Demo
   Witness a Live-Fire Cyber-Attack Simulation in Action!
The U.S. Desperately Needs Cyber Talent

With almost 700,000 cybersecurity job openings, the United States doesn’t have enough cybersecurity experts to protect the nation’s critical infrastructure and federal networks from cyber threats.
Cybersecurity Workforce Gap: 1 in 3 Positions Unfilled

There are only 69 skilled cybersecurity workers for every 100 that employers demand, meaning a shortage of nearly a third of the needed workforce.
The Frequency of All Types of Attacks Against Government Agencies Have Soared

From 2022 to 2023:

- 148% increase in malware attacks
- 51% increase in ransomware incidents
- 37% increase in fileless attacks
- 313% increase in endpoint security incidents (data breaches, unauthorized access, insider threats)
Traditional Cybersecurity Training Methods are Failing

- Foundational training alone fails to equip employees with real-world skills and experience.
- Textbook and rote learning fail to engage employees and nurture knowledge retention.
- Neglecting soft skills fails to develop vital teamwork, communication, and critical thinking skills.
Empowering the Workforce

- On-Demand Learning
- Immersive, Hands-On Experiences in Live-Fire Scenarios
- Alignment with National Cybersecurity Frameworks
- Incentive-Based Skill Development
On-Demand Learning

- **Caters to busy schedules with flexible access.**
- **Promotes** knowledge retention with hands-on learning.
- **Accelerates** capacity to detect and respond to cyber-attacks by making access available from anywhere, at any time.
- **Boosts** retention and engagement with digestible, concentrated messages on current topics.
Hands-On Experience Is Essential to Creating Workforce-Ready Professionals

97% of cybersecurity professionals believe hands-on experience is very important.
Practice Makes Perfect

Companies with an incident response team that also extensively tested their incident response plan experienced $1.49 million less in data breach costs on average than those that had neither measure in place.

Source: IBM 2023
Immersive Live-Fire Cyber-Attack Scenarios: Building Hands-On Experience

Advanced realism and hands-on experience via live-fire exercises develop faster, better incident response capabilities, hone vital soft skills, and prepare teams for real-world attacks.
Alignment with National Cybersecurity Frameworks

Benchmark individual and team progress against industry frameworks to identify knowledge and skill gaps:

- NICE Cybersecurity Workforce Framework Work Roles
- National Institute of Standards and Technology Cybersecurity Framework
- MITRE ATT&CK Frameworks
Incentive-Based Skill Development to Maximize Team Potential:

- Certification programs
- CPE credits
- Shareable badges and rewards
- Customizable competitions
Government Crisis Simulations

- Stress-test crisis management playbooks.
- Increase leadership’s understanding of cyber incidents.
- Hone decision-making and critical-thinking skills.
- Provide hands-on, realistic experience handling crises.
- Boost cross-organizational communication & collaboration.
- Build confidence and resilience in the leadership team.
Address the Challenges:
The Cyberbit Skill Development Platform

Learn the basics
- Cyber Labs: Fundamental skill development

Practice in advanced simulations
- Cyber Range: Live-fire exercises, real-world simulations
- Crisis Simulation: Management-level cyber crisis exercises

Measure your students
- Courses: Beginner to advanced End-to-end curated programs
- Assessment Center: Automated evaluation and progress tracking

Spotlights
- Bite-size videos theoretical content
Let’s See a Live-Fire Cyber Attack Demo!

Thank You
Presentation of FISSEA Security Contest Winners
Presentation of 2024 FISSEA Innovator of the Year

Craig Holcomb
FISSEA Contest and Innovator of the Year Award Lead
FISSEA
Contest and
People’s
Choice Award
Winners
Contest Categories

• Awareness Poster
• Awareness Website
• Awareness Newsletter
• Awareness Video
• Cybersecurity Blog
• Cybersecurity Podcast
• Training Awareness
• Innovative Solutions
Judging criteria

- Judges are not affiliated with any of the groups that submitted entries
- Judges are from various positions and industries
Awareness Poster - Entries

• CenterPoint Energy – “LVL Up Your Defense”
• Newworld – “Orodeus”
• Department of Education – “Beware of Hidden Threats”
• Cofense – “Hollywood Phishing - Credential Phishing (Jurassic Park)”
• Indian Health Service – “Totally Outrageous Cyber Catalog Poster”
Awareness Poster – winner!

• CenterPoint Energy – “LVL Up Your Defense”
Awareness Poster – People’s Choice winner!

- Department of Education – “Beware of Hidden Threats”
Awareness Website

• Indian Health Service – “See Yourself in Cyber”
• GSA – “IDManagement.gov - Modernizing Digital Identity”
• USPS – “Cybersecurity Awareness Month 2022”
• Department of Education – “Cybersecurity Symposium 2023 - Get Your Knowledge #BoostED”
• Cofense – “Phone a Friend”
• FRTIB – “SETA Home Site”
Awareness Website – winner!

- Cofense – “Phone a Friend”
Awareness Website – People’s Choice winner!

- Department of Education – “Cybersecurity Symposium 2023 - Get Your Knowledge #BoostED”
Awareness Newsletter

• Indian Health Service – “Cybersecurity Tools: Your Guide to a Safe School Year”
• Culture Literary International Friends Forum – ”newsletter”
• Cofense – “Awareness Newsletter: Phishing and Microsoft QR Codes”
• FRTIB – “SETA Newsletter”
Awareness Newsletter – winner!

- Indian Health Service – “Cybersecurity Tools: Your Guide to a Safe School Year”
Awareness Newsletter – People’s Choice winner!

• Indian Health Service – “Cybersecurity Tools: Your Guide to a Safe School Year”
Awareness Video

• Indian Health Service – “The Insider Threat at the End of This Video”
• Cofense – “Phishnuts”
• FRTIB – “SETA phishing awareness training video”
Awareness Video – winner!

- FRTIB – “SETA phishing awareness training video”

https://www.youtube.com/watch?v=GH-xc9EYQgk
Awareness Video – People’s Choice winner!

- Cofense – “Phishnuts”
Cybersecurity Blog

- Indian Health Service – “The Jennifer Reacts Blog!”
- Iraje Software Consultants Private Limited – “Cybersecurity Community”
- Department of Education – “Cybersecurity Bits and Bytes”
Cybersecurity Blog – winner!

- Indian Health Service – “The Jennifer Reacts Blog!”
Cybersecurity Blog – People’s Choice winner!

• Department of Education – “Cybersecurity Bits and Bytes”
Cybersecurity Podcast

• No entries!
Training Awareness

• Indian Health Service – “An Insider Threat at IHS”
• CenterPoint Energy – “Cybersecurity Awareness- Safety Phishing Training”
• Department of Education – “Information Guardians: Immersive Storytelling in Web-based Training”
Training Awareness – winner!

• Indian Health Service – “An Insider Threat at IHS”

https://www.youtube.com/watch?v=DUhyWqVLN5Q
Training Awareness – People’s Choice winner!

- Department of Education – “Information Guardians: Immersive Storytelling in Web-based Training”
Innovative Solutions

- Indian Health Service – “Multi-Factor Authentication-Zee”
- Social Security Administration – “SSA’s Phish Your Colleague” Cybersecurity Awareness Month Program
- Nanoforz – “Abercrombie&Forz”
- USPS – “Smart Cybersecurity Moment slides”
- Department of Education – “Cyber Badging Program: Friendly Competition Driving Behavioral Change”
- Cofense – “QR Code Simulations and Education”
Innovative Solutions – winner!

- Indian Health Service – “Multi-Factor Authentication-Zee”
Innovative Solutions – People’s Choice winner!

- Social Security Administration – “SSA’s Phish Your Colleague” Cybersecurity Awareness Month Program

About Phish Your Colleague
The 2024 FISSEA Cybersecurity Awareness and Training Innovator of the Year is....

It was a close race so...
The 2024 FISSEA Cybersecurity Awareness and Training Innovator of the Year is

Oz Alashe
CEO and Founder of CybSafe
And the 2024 FISSEA Cybersecurity Awareness and Training Innovator of the Year Runner Up is:

**William D. Cosner**

Cybersecurity Assessment Team Chief
Defense Contract Management Agency, Defense Industrial Base Cybersecurity Assessment Center
Thank you to all the wonderful entrants!

Thank you to our judges!
Closing Remarks

Marian Merritt
Deputy Director NICE
National Institute of Standards and Technology

Brooke Crisp
FISSEA Co-Chair

Frauke Steinmeier
FISSEA Co-Chair

#FISSEA | nist.gov/fissea
THANK YOU FOR ATTENDING
34th ANNUAL FISSEA CONFERENCE!

We look forward to receiving your feedback via the post-event survey!

https://www.surveymonkey.com/r/34thAnnualFISSEAConference

#FISSEA | nist.gov/fissea
Get Involved

Subscribe to the FISSEA Mailing List
FISSEAUpdates@list.nist.gov

Volunteer for the Planning Committee
https://www.nist.gov/itl/applied-cybersecurity/fissea/meet-fissea-planning-committee

Serve on the Contest or Award Committees for 2025
Email fissea@list.nist.gov

Submit a presentation proposal for a future FISSEA Conference or FISSEA Forum
https://www.surveymonkey.com/r/fisseacallforpresentations

#FISSEA | nist.gov/fissea