FISSEA Winter Forum

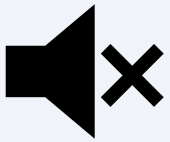
February 10, 2026

1:00pm – 2:30pm ET

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

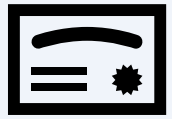
Notes and Reminders



Attendees are muted: Due to the number of attendees, all participant microphones and cameras are automatically muted.

Webinar Recording: This webinar and the engagement tools will be recorded. An archive will be available at www.nist.gov/fissea.

Submitting Questions: Please enter questions and comments for presenters in the Zoom for Government Q&A. Chat has been disabled for this event.



CE/CPE credits: The CEU form will be available on the event page after the event.

Welcome and Opening Remarks

Joyce Mui
FISSEA Co-Chair
University of Maryland Medical System &
University of Maryland Institute for
Health Computing

Danielle Santos
Deputy Director of NICE
National Institute of Standards and
Technology, U.S. Department of Commerce

Get Involved

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

Serve on the Contest or Innovator of the Year Committees
Email fissea@nist.gov

Submit a proposal to speak at a future FISSEA event.
https://survey.nist.gov/jfe/form/SV_dmy6dxR2mPY4udU

SAVE THE DATE

Federal Information Security Educators (FISSEA) Spring Forum

May 12, 2026

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

FISSEA Fifteen: A Collaborative Discussion on Cybersecurity Awareness Activities

Susan Hansche

Training Manager
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FISSEA 15
Winter Forum 2026
Interactive Questions

What training topics are you interested in or need additional skill development?

What training topics do you think your audience needs?

Training - this is about your training needs

I'm constantly asking coworkers for help because I wasn't trained.

Where do I fit in?

I want to grow at work, but I haven't been trained enough to take on new responsibilities.

The initial training was okay, but I haven't received any updates or new skills training since then.

There are changes happening at work, but no one is training us on how to adapt.

How am I supposed to know this?

I'm not sure what's expected of me or how to fully perform my job responsibilities.

Is this what I'm supposed to be doing?

I don't feel like I'm set up for success here.

I spend so much time teaching myself how to do it.

I was thrown into the role without any preparation.

The training was rushed and didn't cover everything I need to know.

It feels like they don't care whether I succeed or not if they won't invest in my training.

So glad I can look it up on ChatGPT

What training do you need?
What topic would you like to know more about?

Cybersecurity Topics

- ChatGPT or Generative AI
- Cloud Security
- Mobile Device Security
- Current Threats

Management Topics

- Great communication skills
- Better writing for work
- Supervising
- Program Management

Awareness & Training Topics

- Awareness Month Ideas
- Writing learning objectives
- Creating interactive learning activities
- Managing the training budget
- Promoting training needs to leadership
- Return on investment?
- Using metrics to advance programs

What training does your audience need? What topic is your audience asking for?

What am I supposed to be doing with AI?

I'm not very good at uploading docs to the right Sharepoint site, where is this supposed to be filed?

I was just assigned an ancillary duty to manage the awareness program. What do I do now?

How do you maintain an Authority to Operate?

I can't believe they are moving to a SaaS solution. Where is the security there?

You want me to go through the logs and find something? What was it again?

What exactly is an ISSO?

What do you mean, there are over 1,000 controls?

I wish I was more creative in my awareness program!

Interactive Sharing Time

(look for the link in chat and follow Danielle's instructions
or just use chat to write a response)

What training topics are you interested in or need additional skill development?

What training topics do you think your audience needs?

General Public (Mis)Understanding of Common Cybersecurity Terms

Julie Haney

Computer Scientist and Lead for the
Human-Centered Cybersecurity Program
National Institute of Standards and Technology

General Public (Mis)Understanding of Common Cybersecurity Terms

Julie Haney, Yee-Yin Choong,
Sandra Spickard Prettyman, Kristin Koskey, Simon Wang

February 10, 2026

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

The Jargon Problem

- Scientific/technical jargon (terms) can negatively impact:
  - ability to process and understand information
  - interest in the subject
  - support for or willingness to use emerging technologies
  - relationships between non-expert and expert groups

Do you know how well your employees understand cybersecurity jargon?

Study Purpose

To explore the general public's familiarity and understandings of common cybersecurity terms.

To identify potential influences of generation (age group), education level, and term category (Defense terms vs. Threat terms)

Common Cybersecurity Terms

Defense Terms

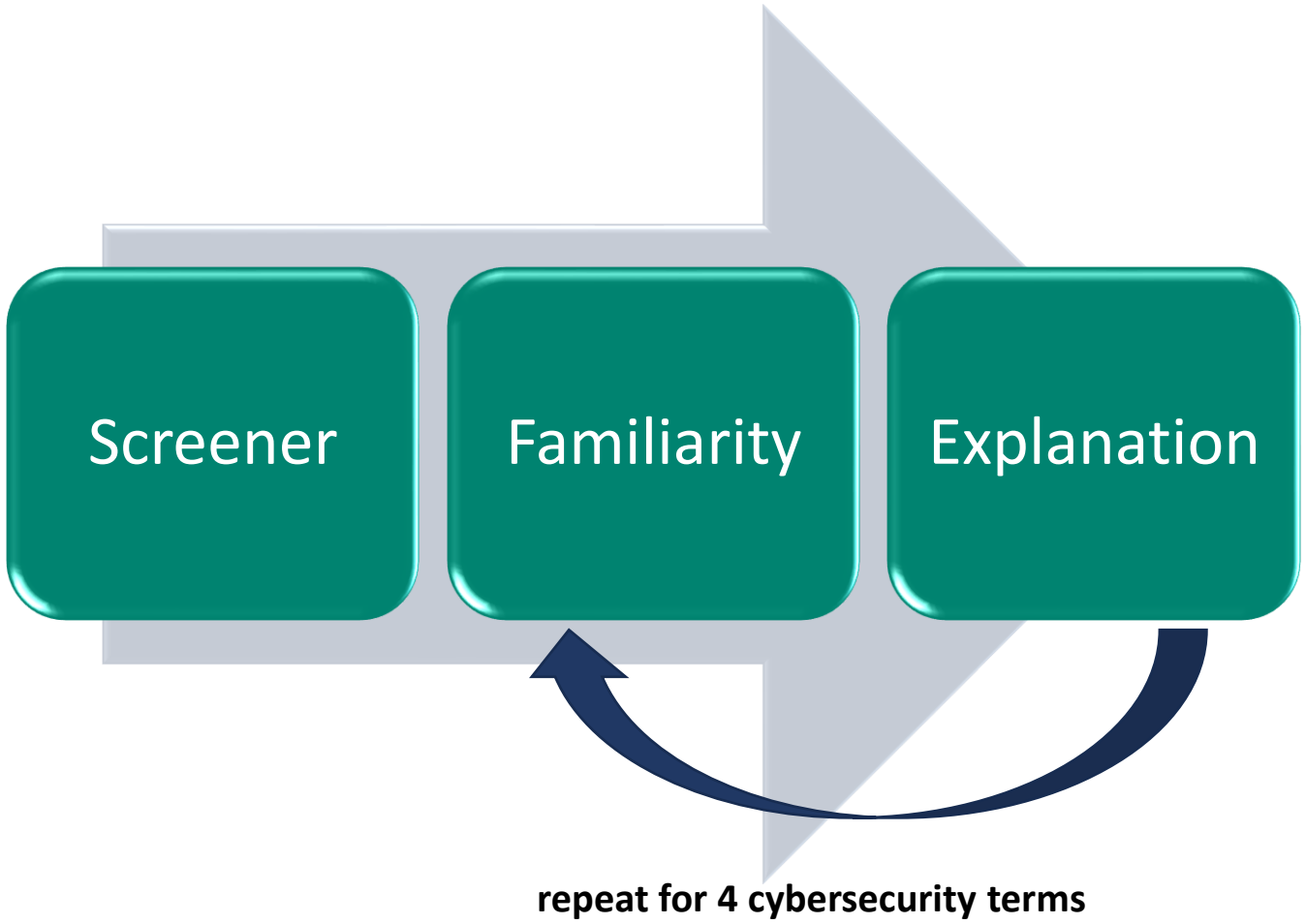
- antivirus
- cryptography
- cybersecurity
- encryption
- ethical hacker
- firewall
- information security
- intrusion detection
- multi-factor authentication
- patch
- penetration testing
- VPN

Threat Terms

- advanced persistent threat
- botnet
- data breach
- distributed denial of service (DDoS)
- hacker
- malware
- phishing
- ransomware
- social engineering
- spyware
- trojan horse
- zero-day

Survey

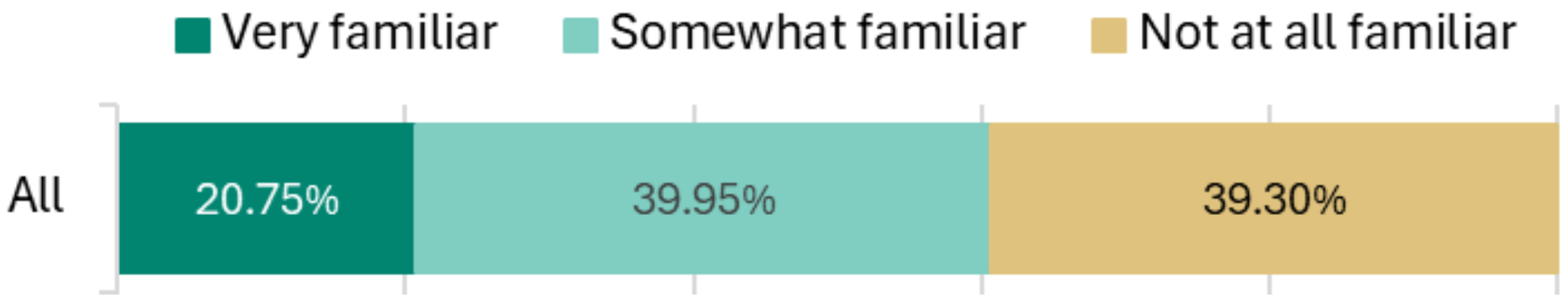
- 6 survey versions, 4 terms in each
- Each version completed by 108-114 participants (659 total)
- Participants (roughly) representative of U.S. adult population for generation and education level



Familiarity and Level of Understanding

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Familiarity



Participants were significantly more familiar with Defense terms as compared to Threat terms

Familiarity: Individual Terms

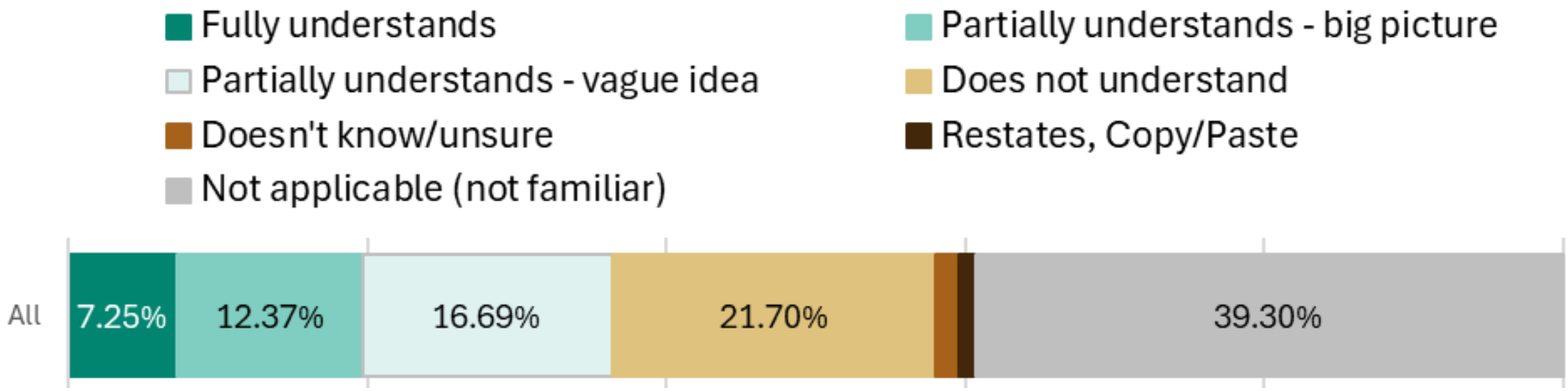
Most familiar (at least 80%)

- antivirus
- cybersecurity
- multi-factor authentication
- encryption
- firewall
- hacker
- data breach
- malware
- spyware

Least familiar (less than 25%)

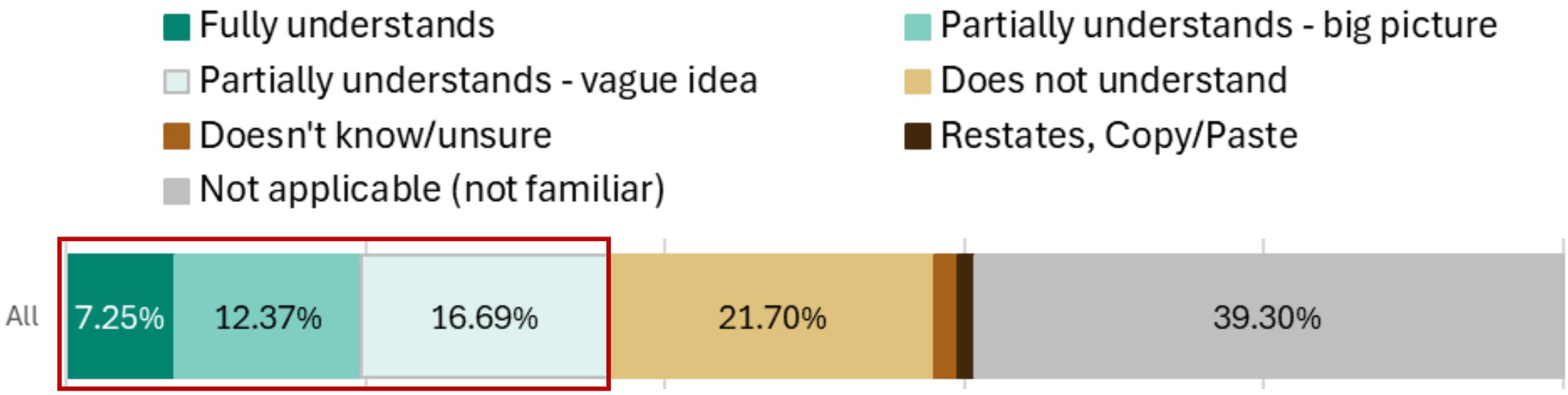
- cryptography
- penetration testing
- distributed denial of service
- zero-day
- botnet

Level of Understanding (LOU)



Higher familiarity was correlated with higher LOU for Defense, but not Threat, terms.

Level of Understanding (LOU)



Higher familiarity was correlated with higher LOU for Defense, but not Threat, terms.

Level of Understanding: Individual Terms

Highest LOU (at least 50%)

- antivirus
- cybersecurity
- multi-factor authentication
- hacker
- data breach
- malware
- phishing

Lowest LOU (less than 20%)

- firewall
- cryptography
- ethical hacker
- penetration testing
- distributed denial of service
- advanced persistent threat
- social engineering
- botnet
- zero-day

Misconceptions & Misapplications (M&M)

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

M&M: Scope

Too narrow	Overly generic	Vague
hacker: *“Someone has access to your accounts”*	firewall: *“protection of a computer device”*	ransomware: *“take over control of something”*

M&M: Conceptual/Factual

Good vs. bad

spyware:
"an app to protect your privacy"

Everything's a virus

malware:
"some type of virus"

Equating to another term

VPN:
"it is an identifying feature for an online device"

More Conceptual errors for Threat terms as compared to Defense terms

M&M: Contextual

Different/wrong context

patch:
"To place something over top of an existing object for strength, stability and durability"

Externalization

cybersecurity:
"A company or service that keeps your computer information secure"

No mention of tech/online

phishing:
"when someone contacts you pretending to be someone that needs your financial information for some reason"

More Contextual errors for Threat terms as compared to Defense terms

Demographic Differences

Participants with Bachelor's+ education had:

- higher levels of Familiarity
- higher Levels of Understanding
- fewer Conceptual errors

Generational differences only found for individual terms, for example:

- Baby Boomers had less Familiarity with ***VPN*** and ***hacker*** compared to Gen Z
- Baby Boomers had lower LOU for ***social engineering*** compared to Millennials

Implications for Communicating Concepts

Avoid assumptions

Focus on relevance

Communicate scope

Map threats to defenses

Tailor & prioritize

Questions?

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

FISSEA Ignite!: From Compliance to Confidence: Teaching Cyber Risk Through Data Trust

Rajesh Vayyala
Principal Data Architect
Independent Researcher

From Compliance to Confidence

Teaching Cyber Risk Through Data Trust

FISSEA Winter Forum: February 10, 2026

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Rajesh Vayyala
Principal Data Architect

The Compliance Paradox

We train people to **follow rules**...

But real threats require **critical thinking**

85%

of breaches involve human error, yet compliance training hasn't reduced this number

Source: Verizon Data Breach Investigations Report – ~85% of breaches involve a human element.

What is Data Trust?

Data trust is the confidence that comes from understanding the value, sensitivity, and proper handling of information

Value Recognition

Understanding what data matters and why it needs protection

Risk Awareness

Recognizing threats in context, not just following rules

Ownership Mindset

Feeling personally responsible for organizational data

Teaching Data Trust

Moving from Abstract Rules to Concrete Context

Compliance Approach

- Never click suspicious links
- Always use strong passwords
- Report incidents within 24 hours
- Focus on what to do, not why

Data Trust Approach

- Here’s how attackers exploit trust and human behavior
- This data contains 10K SSNs, here’s the potential breach cost
- When in doubt, you have the authority to pause and verify
- Password rules → Understanding how credential theft leads to account takeover and data loss

Three Methods to Build Data Trust

1 

Data Value Mapping

Help employees classify and understand the data they handle daily

2 

Threat Simulation with Context

Go beyond phishing tests explain the attack chain and business impact

3 

Scenario-Based Decision Making

Use realistic cases where employees must weigh risk and make judgment calls

The Impact

Organizations that shift to data-trust-based training see measurable behavior change

40%

Increase in threat reporting

60%

Reduction in successful phishing

3x

Higher training engagement

85%

Employee confidence in security decisions

Illustrative ranges based on security awareness and phishing training studies (e.g., Hoxhunt, Keepnet Labs, SoSafe).

Getting Started

Audit your current training
Does it explain WHY or just WHAT? Where can you add context?

Start small with one team
Pilot a data value mapping exercise or scenario-based workshop

Measure understanding, not just completion
Can employees explain the 'why' behind security practices?

Iterate based on feedback
Let employees shape the training they know what resonates

From Compliance to Confidence

*When we trust our people with **knowledge**,*
they become our strongest defense.

Questions?

Rajesh Vayyala
vayyalarajesh.com
https://www.linkedin.com/in/rajeshvayyala/

Field-Tested AI Tactics: Building Better Cybersecurity Assessments with Generative Tools

Jim Wiggins

CEO

Federal IT Security Institute (FITSI)

Field-Tested AI Tactics: Building Better Cybersecurity Assessments with Generative Tools

Jim Wiggins
Chief Executive Officer
Federal IT Security Institute

FISSEA Winter Forum
Date: 02/10/26

FITSI
FEDERAL IT SECURITY INSTITUTE
HELPING SECURE THE NATION'S FEDERAL INFORMATION SYSTEMS

Agenda

- Introduction
- Why This Matters Now
- The Reality of Assessment Design
- Where Generative AI Fits
- Bounded Roles for AI in Assessments
- Tactic #1: Prompted Scenario Ideation
- Tactic #2: Enforcing Cognitive Rigor
- Tactic #3: Better Distractors at Scale
- Tactic #4: Framework Mapping Support
- Prompting That Actually Works
- Iterative Prompt Chains
- Guardrails & Risk Management
- Accreditation & Defensibility Considerations
- What Worked / What Didn’t
- Key Takeaways & Closing Q&A
- Q&A
- Contact Information

Introduction

- Chief Executive Officer of the Federal IT Security Institute
- Cybersecurity Trainer and Information Security Practitioner
- 29 of experience in IT
- 24 of experience in IT security
- 3 years of experience in Generative AI
  - Trained Over 1500 Students in Generative AI
    - 500+ National Risk Management Center
    - 400+ Defense Information Systems Agency
    - 300+ Department of Interior
    - 300+ ISACA Chapter
- Has a Masters in Assessment Testing and Measurement in Education from GWU

Why This Matters Now

- The Assessment Pressure Point
  - Growing demand for cybersecurity talent
  - SME scarcity and burnout
  - Rising expectations for rigor and defensibility
  - Time-to-market pressure

The Reality of Assessment Design

- What Makes Cybersecurity Assessments Hard
  - Scenario realism
  - Cognitive rigor (decision-making vs recall)
  - Framework alignment (NIST, 8140, ISO)
  - Consistency across items and forms

Where Generative AI Fits

- AI as a Force Multiplier - Not an Author
  - What AI can do:
    - Accelerate ideation
    - Enforce structure
    - Expand scenario space
  - What AI cannot do:
    - Determine correctness
    - Replace SMEs
    - Ensure compliance on its own

Bounded Roles for AI in Assessments

- Defined, Defensible Use Cases
  - Scenario stem generation
  - Distractor ideation
  - Cognitive-level elevation
  - Framework mapping assistance

Tactic #1: Prompted Scenario Ideation

- Breaking the Blank Page Problem
  - Generate:
    - Realistic operating contexts
    - Constraints and pressures
    - Role-specific situations
  - SME selects, edits, validates

Tactic #2: Enforcing Cognitive Rigor

- Moving Beyond Recall
  - Using prompts to:
    - Detect recall-level questions
    - Rewrite to decision-based items
    - Introduce tradeoffs and risk
    - Aligning with Bloom's levels

Tactic #3: Better Distractors at Scale

- Why Bad Distractors Kill Good Questions
  - Common SME pitfalls:
    - Obviously wrong answers
    - Policy trivia
  - AI use:
    - Generate plausible but incorrect options
    - Vary misconception types

Tactic #4: Framework Mapping Support

- Traceability Without the Tedium
  - AI assists with:
    - Mapping to NIST SP 800-53 / 800-37
    - Role/task alignment (DoD 8140)
  - Human validation remains mandatory

Prompting That Actually Works

- Field-Tested Prompt Design
  - Role-conditioned prompts
  - Environment constraints (Federal, classified, cloud)
  - Explicit exclusions (“Do not reference vendors”)

Iterative Prompt Chains

- Draft → Critique → Refine
  - Separate prompts for:
    - Stem quality
    - Cognitive level
    - Distractor quality
  - Improves consistency and review speed

Guardrails & Risk Management

- What Can Go Wrong - and How We Mitigate It
  - Risks:
    - Hallucination
    - Overconfidence bias
    - Hidden assumptions
  - Controls:
    - SME-in-the-loop
    - Source anchoring
    - Prompt templates

Accreditation & Defensibility Considerations

- AI Use in an Oversight Environment
  - Human judgment remains authoritative
  - Version control and documentation
  - Auditability of the development process

What Worked / What Didn’t

- Lessons from Real Use
  - Worked well:
    - Scenario diversity
    - Cognitive uplift
    - Faster development cycles
  - Didn’t work:
    - Unconstrained generation
    - “One-prompt solutions”
    - Skipping SME review

Key Takeaways & Closing Q&A

- Three Things to Remember
  - Constrained AI improves assessment quality
  - SMEs remain essential - AI accelerates them
  - Governance matters more than tooling

Q&A

Contact Information

- Jim Wiggins
  - Email: jim.wiggins@fitsi.org
  - Phone: 703-828-1196 x701
  - Cell: 571-277-4661

Recap

- Introduction
- Why This Matters Now
- The Reality of Assessment Design
- Where Generative AI Fits
- Bounded Roles for AI in Assessments
- Tactic #1: Prompted Scenario Ideation
- Tactic #2: Enforcing Cognitive Rigor
- Tactic #3: Better Distractors at Scale
- Tactic #4: Framework Mapping Support
- Prompting That Actually Works
- Iterative Prompt Chains
- Guardrails & Risk Management
- Accreditation & Defensibility Considerations
- What Worked / What Didn’t
- Key Takeaways & Closing Q&A
- Q&A
- Contact Information

Closing Remarks

Latha Reddy
FISSEA Co-Chair
Spire Investment Partners, LLC

THANK YOU

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

https://survey.nist.gov/jfe/form/SV_afO3TG6G2tp5GvA

#FISSEA | nist.gov/fissea

Get Involved

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

Serve on the Contest or Innovator of the Year Committees
Email fissea@nist.gov

Submit a proposal to speak at a future FISSEA event.
https://survey.nist.gov/jfe/form/SV_dmy6dxR2mPY4udU

FISSEA Contest

Six Contest Categories

- Poster or Brochure
- Website
- Multimedia
- Email Campaign and/or Newsletter
- Miscellaneous
- Most Innovative Solution

Contest entries must be unclassified and approved to be shared publicly.

Submission Deadline: March 27, 2026, at 11:59pm ET

FISSEA Innovator of the Year

Nominees may include, but are not limited to:

- Cyber Instructional Curriculum Developers
- Cybersecurity Instructors
- Cybersecurity Program Managers
- Workforce Development Managers
- Practitioners Who Further Awareness and Training Activities or Programs

Nominees can be Federal Employees or Contractors directly supporting Federal Employees.

Submission Deadline: March 27, 2026, at 11:59pm ET

SAVE THE DATE

Federal Information Security Educators (FISSEA) Spring Forum

May 12, 2026

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA