



INCREASING CYBERSECURITY AWARENESS

THE HUMAN FIREWALL

Federal Information Security Educators (FISSEA)

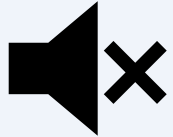
Fall Forum

September 15, 2026

1:00 p.m. – 3:00 p.m. ET

#FISSEA | nist.gov/fissea

Notes and Reminders



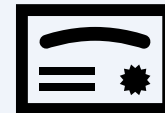
Attendees are muted: Due to the number of attendees, all participant microphones and cameras are automatically muted.



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



Danielle Santos

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



Karen Bovell

FISSEA Co-Chair
Education Program Specialist, Employee
Experience & Workforce Development,
Orlando VA Healthcare System

NIST plans to develop practical and actionable guidelines to help organizations take a human-centered approach in their cybersecurity programs.

We need your help determining the way forward!

Read our **Human-Centered Cybersecurity Concept Paper**
available at:

<https://csrc.nist.gov/projects/human-centered-cybersecurity>

Email your feedback to human-cybersec@nist.gov
by **September 30, 2026**.



NIST Human-Centered
Cybersecurity website

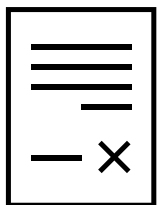
CYBERSECURITY CAREER WEEK

OCTOBER 19 – 24, 2026

#CyberCareerWeek #MyCyberJob #ChooseCyber

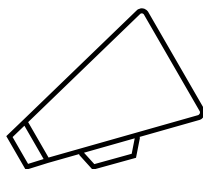


Call for Commitments



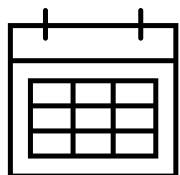
Submit a Proclamation

Official statements from governments, leadership, or schools.



Spread Awareness

Share career kits, NICE Framework tools, & engage via social media platforms.



Host an Event

Career fairs, open houses, webinars, workshops, or job shadowing.



Classroom Speaking

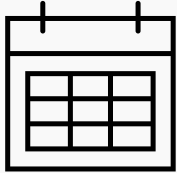
Present at panels or guest lecture on cyber career pathways.

Pledge Your Support!

Add your activity to the event map and help spark the future cybersecurity workforce!

nist.gov/ccw-event-activity-portal

CCW Events & Activities



2026 Cybersecurity Career Week event held by SANS in coordination with NICE

Tuesday, September 22, 2026 | 2:30 - 6:00 PM ET

Location: U.S. Capitol Visitors Center, SVC 212-10

**Register by Sept 18*

Networking Like a Leader: Building Authentic Connections That Create Opportunities

October 14, 2026 | 1:00 - 2:00 PM ET

Challenge: Six Day #mycyberjob Media Challenge

October 19-24, 2026

X, Instagram, Facebook, LinkedIn and other

Tag: @NISTCyber

X Chat: NIST Chat #CyberCareerChat #CyberCareerWeek #MyCyberJob

October 19, 2026 | 12:00 - 12:30 PM ET

Breaking Into Cybersecurity: Real Stories from Recent Graduates (Webinar)

October 20, 2026 | 1:00 - 2:00 PM ET

NICE Webinar: Helping to Chart the Course - Unlocking Student Pathways into Cybersecurity Careers

October 21, 2026 | 1:00 - 2:00 PM ET

Cyber Career Realities Revealed: Panel Across NICE Framework Work Role Categories

October 22, 2026 | 1:00 - 2:00 PM ET

nist.gov/nice/ccw

CCW is supported by the NICE Program Office at NIST.

Get Involved



Subscribe to the FISSEA Mailing List
FISSEAUUpdates+subscribe@list.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) Winter Forum**

February 9, 2027

#FISSEA | nist.gov/fissea

Opening Keynote - Securing the Next 250

Jeanie Moore

Associate Chief, Strategic Communication, Office of the
Chief External Affairs Officer, Cybersecurity and
Infrastructure Security Agency



SECURING *THE* *NEXT* **250**

cisa.gov/cybersecurity-awareness-month



**CYBERSECURITY
AWARENESS
MONTH**

OCTOBER 2026

How We Got Here



**CYBERSECURITY
AWARENESS
MONTH**
OCTOBER 2026

Cybersecurity Awareness Month

Securing the Next 250

October is Cybersecurity Awareness Month!

Cyber threats are getting faster and smarter. New and evolving technology, such as [Artificial Intelligence](#) is accelerating the rate at which hackers can find and take advantage of weak spots in our computer software and systems. That puts our country and economy at risk.

But we can fight back. We encourage everyone to explore the tips and resources on this page.

Secure Your Organization

This Cybersecurity Awareness Month, commit to having better cybersecurity in your communities and critical infrastructure.

Secure Your Business

Secure State, Local, Tribal and
Territorial Government

- **2025 – First major updates in over 20 years**
 - Shift focus to SMB and SLTT entities
 - Expand on the basic 4 steps

What Makes This Year Different



**CYBERSECURITY
AWARENESS
MONTH**
OCTOBER 2026

- **New Audience**
- **2 new steps:**
 - Have an incident response plan
 - Prepare for system disruption

Secure Critical Infrastructure

Reduce, Replace, Recover: Secure Critical Infrastructure Systems, Data and Services from Online Threats

Secure Critical Infrastructure to Secure the Nation

Today's critical infrastructure relies heavily on systems and devices that are connected to the Internet. While this improves efficiency, it also exposes critical infrastructure to attempts to infiltrate systems, data, and other sensitive information by malicious actors—often backed by hostile foreign nations. In fact, many critical infrastructure systems have already been compromised but may not know it yet.

Securing Critical Infrastructure

The threat landscape is fundamentally changing. IT's scaling—dramatically. Accelerated by artificial intelligence (AI) advancements, the discovery and exploitation is unprecedented. By August 2025, the number of vulnerabilities added to the Common Vulnerabilities and Exposures (CVE) list surpassed the total recorded for all of 2025. Every organization has the power to strengthen America's cybersecurity.

This Cybersecurity Awareness Month, we invite you to join us in practicing the 3Rs of Cybersecurity: **Reduce, Replace, Recover**. With the cyber resilience America.

Additional Steps You Can Take

1. **Reduce Cyber Incident Impact:** Implement a robust incident response plan, including a dedicated incident response team, to quickly identify, contain, and recover from cyber incidents.
2. **Replace Vulnerable Systems and Data:** Regularly update software, hardware, and data to the latest versions, ensuring they are secure and free from known vulnerabilities.
3. **Recover from Cyber Incidents:** Develop and test a disaster recovery plan to ensure critical systems and data can be restored quickly and accurately after a cyber incident.



For critical infrastructure agencies, CI Fortify is a framework for identifying, assessing, and reducing risks to the security and resilience of critical infrastructure systems and data.

1. **Identify:** Identify the critical infrastructure systems and data that are most vulnerable to cyber threats.
2. **Assess:** Assess the risk to the critical infrastructure systems and data from cyber threats.
3. **Reduce:** Reduce the risk to the critical infrastructure systems and data by implementing security measures.
4. **Recover:** Recover from cyber incidents by implementing a disaster recovery plan.

Leadership Sets the Tone for a Culture of Cybersecurity

As a critical infrastructure leader, your commitment to cybersecurity sets the tone for your entire organization. Implementing our own cybersecurity best practices will make

Building Cyber Maturity



**CYBERSECURITY
AWARENESS
MONTH**
OCTOBER 2026

- **The Four Core**

- Avoid and report phishing scams.
- Use strong passwords.
- Use multifactor authentication and a password manager.
- Update software.

Building Cyber Maturity (cont'd)



**CYBERSECURITY
AWARENESS
MONTH**
OCTOBER 2026

- **Five More**

- Use logging on your systems
- Back up data
- Encrypt data
- Get a .gov domain if eligible
- Report cyber incidents to CISA

- **And Two New**

- Have an incident response plan and use it
- Be prepared for system disruptions

Easy Ways to Participate in CAM



**CYBERSECURITY
AWARENESS
MONTH**
OCTOBER 2026



Tools & Samples

The [Cybersecurity Awareness Month 2026 Toolkit](#) has ready-to-go and customizable tools and templates to help you conduct your campaign. Be sure to check back regularly as we add new tools!

Email Signature Banner

Encourage leaders and influencers in your organization to use this image in their email signatures all month long. Use the full-size PNG file in the toolkit, copying the thumbnail below.



Virtual Backgrounds

PowerPoint Presentations

Social Media Suggestions

Posters

Tip Sheets



- Email to employees, customers, vendors
- Signature Block Graphic
- Print our Posters
- Share Printable Tip Sheets

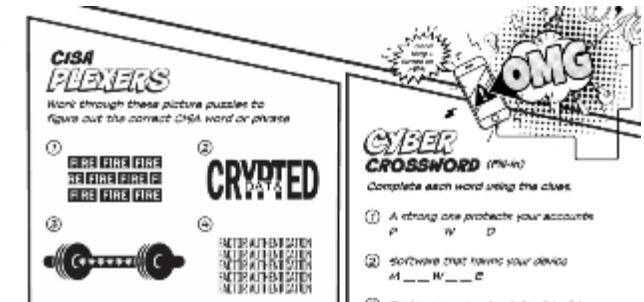
▪ www.cisa.gov/cybersecurity-awareness-month

More Ways to Get Involved



**CYBERSECURITY
AWARENESS
MONTH**
OCTOBER 2026

- Info booth
- Posters
- Guided discussions
- Games
- Webinars
- Celebrate Cyber Careers Week!



Getting Leadership Support



**CYBERSECURITY
AWARENESS
MONTH**
OCTOBER 2026

Cybersecurity Best Practices For [your organization's name]

Create a Culture of Cybersecurity



CYBERSECURITY
AWARENESS
MONTH
OCTOBER 2026

Cybersecurity is a culture, not just a checklist.

A strong cybersecurity culture includes clear policies, regular employee training, and engagement from IT and leadership. It also means ensuring that partners and vendors follow strong security practices.

DISCUSSION

Do we have an organization-wide cybersecurity policy in place? Is it followed consistently?
Are we holding our partners and vendors to the same standards?

Four Cybersecurity Essentials



CYBERSECURITY
AWARENESS
MONTH
OCTOBER 2026

The following four practices are the foundation of organizational cybersecurity and should be as automatic as buckling a seatbelt:



Teach employees to avoid phishing

Recognizing and reporting suspicious emails and links may prevent cyber attacks.



Require strong passwords

Long, random, unique passwords make accounts harder to breach.



Require multifactor authentication

Adds an extra layer of protection if a password is compromised.



Update software

Keeps systems protected against known vulnerabilities.

DISCUSSION

Are we doing it
Is there room for improvement?

New Actions for 2026



CYBERSECURITY
AWARENESS
MONTH
OCTOBER 2026

New actions for 2026 (Cyber Performance Goals):

- **Have an Incident Response plan (IR) and use it!** Organizations should develop, maintain, update, and regularly exercise IR plans for common threat scenarios such as ransomware attacks. Ensure drills are realistic and include all relevant stakeholders, such as organizational leadership and legal counsel, in addition to technical personnel. IR plans should be reviewed and drilled on an annual basis at a minimum.
- **Be prepared for system disruptions.** Organizations should develop and execute plans to recover and restore service to critical assets or systems that might be impacted by a cybersecurity incident. Consider including the ability to execute mission essential functions without access to critical assets or even internet access (e.g., shift to paper-based operations, radio communications, etc.)

DISCUSSION

Do you have an incident response plan?
When was the last time your plan was tested and/or updated?
Do you know what to do during a major disruption without power?

SECURING THE NEXT **250**



**CYBERSECURITY
AWARENESS
MONTH**
OCTOBER 2026

cisa.gov/cybersecurity-awareness-month

Contact us

CISA-ExternalAffairs@cisa.dhs.gov

Q&A

Are There Any Questions?

FISSEA Fifteen: Let's Build a Micro-Training Module

Susan Hansche

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



Polls

Choose the Training Topic and Audience



BREAK

We will resume promptly at 2:00 p.m. ET

Welcome Back

Joyce Mui

FISSEA Co-Chair, Senior Manager Research Informatics,
University of Maryland Medical System & University of
Maryland Institute for Health Computing



Featured Panel: Using the NICE Framework in Cybersecurity Learning



Brittney Thomas

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



Dr. Natalie Foster Johnson

Founder and Researcher
CyberMINDS Research Institute

Level Up: Applying Cybersecurity Skills Through the President's Cup Competition and Practice Area

Brittney Thomas

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





PRESIDENT'S CUP

CYBERSECURITY
COMPETITION

WELCOME TO President's Cup 8

- Competition Overview
- Participation Benefits
- Competition Structure, Key Dates, and Timeline
- Hack of Fame
- President's Cup Resources



PRESIDENT'S CUP

CYBERSECURITY COMPETITION

Designed to identify, challenge, and reward the top cybersecurity talent in the federal workforce.

Established by America's Cybersecurity Workforce E.O. 13870 and authorized by FY23 NDAA allowing CISA to hold the annual competition.



Competition Structure

3

TRACKS

Individuals Defensive
Individuals Offensive
Teams

Competition Eligibility

Federal Employees, Active Duty Military, and Reservists can register and compete.

Contractors are Ineligible

3

ROUNDS

2 Virtual Qualifying Rounds
In Person Finals

Practice Resources

Practice Area and Game of the Month participation is publicly available to anyone



Participation Benefits



SKILL DEVELOPMENT

Hands-on experience in
cybersecurity
NICE Framework alignment for
you and your team



CONTINUOUS LEARNING

Access to past
challenges and resources
to train as roles evolve



CAREER ADVANCEMENT

Build your professional
network and represent your
agency at the national scale

Hack of Fame



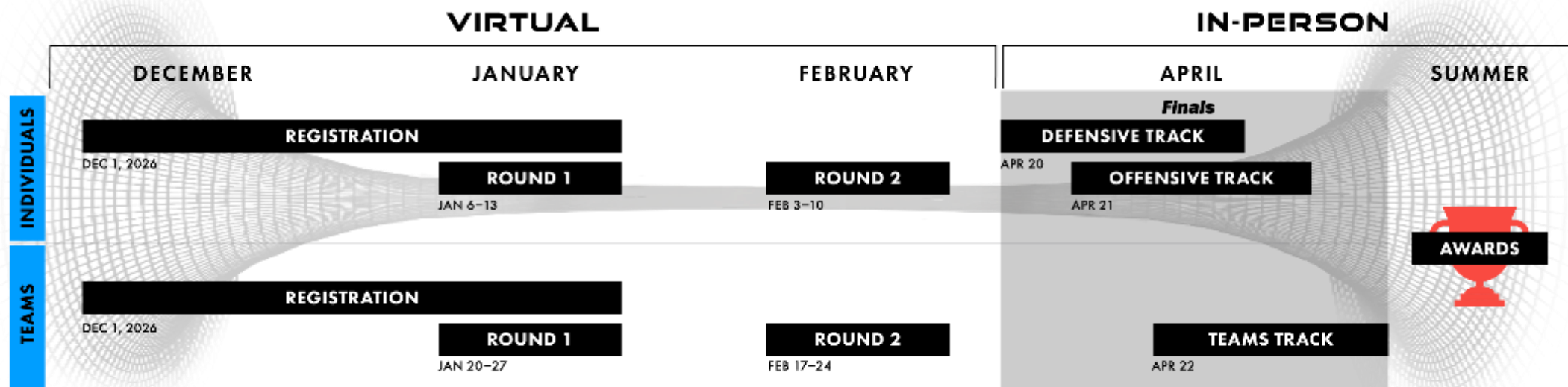
- Recognizing elite performers from PC1 moving forward with at least one first place finish among their 3 top 3 placements.
- Provides continued engagement opportunities through mentorship, challenge development, panel participation, exhibition-based competitions, and red team activities.
- Eligibility cap applies after three top-three finishes, including one first-place win (PC7 moving forward).



PC8

SANDS OF TIME

America's 250 Years of Technology



REGISTRATION OPENS DECEMBER 1, 2026



PREPARE FOR PC8

Year Round Resources

PRACTICE AREA

Open access to past challenges and solution guides for training and skill development.

WORKSHOPS & MINI COMPETITIONS

Providing hands-on experiences for your teams to train and collaborate.

GAME OF THE MONTH

Monthly, real-world cyber scenarios tied to NICE work roles allowing participants to build skills.

CPU/CPE CERTIFICATES

Recognition and certificates for participation and skill achievement, CPU/CPE credit.

GITHUB REPOSITORY

Publicly available challenge materials and educational resources.



PRESIDENT'S CUP

CYBERSECURITY
COMPETITION



TURN PRACTICE INTO PERFORMANCE

cisa.gov/prescup

PRESIDENTSCUP@CISA.DHS.GOV





PRESIDENT'S CUP

CYBERSECURITY
COMPETITION



Q&A

Are There Any Questions?

Using Storytelling and Comic Characters to Teach the NICE Workforce Framework: The Resilience Lab Approach

Dr. Natalie Foster Johnson

Founder and Researcher
CyberMINDS Research Institute



THE RESILIENCE LAB COMIC SUPER HEROS

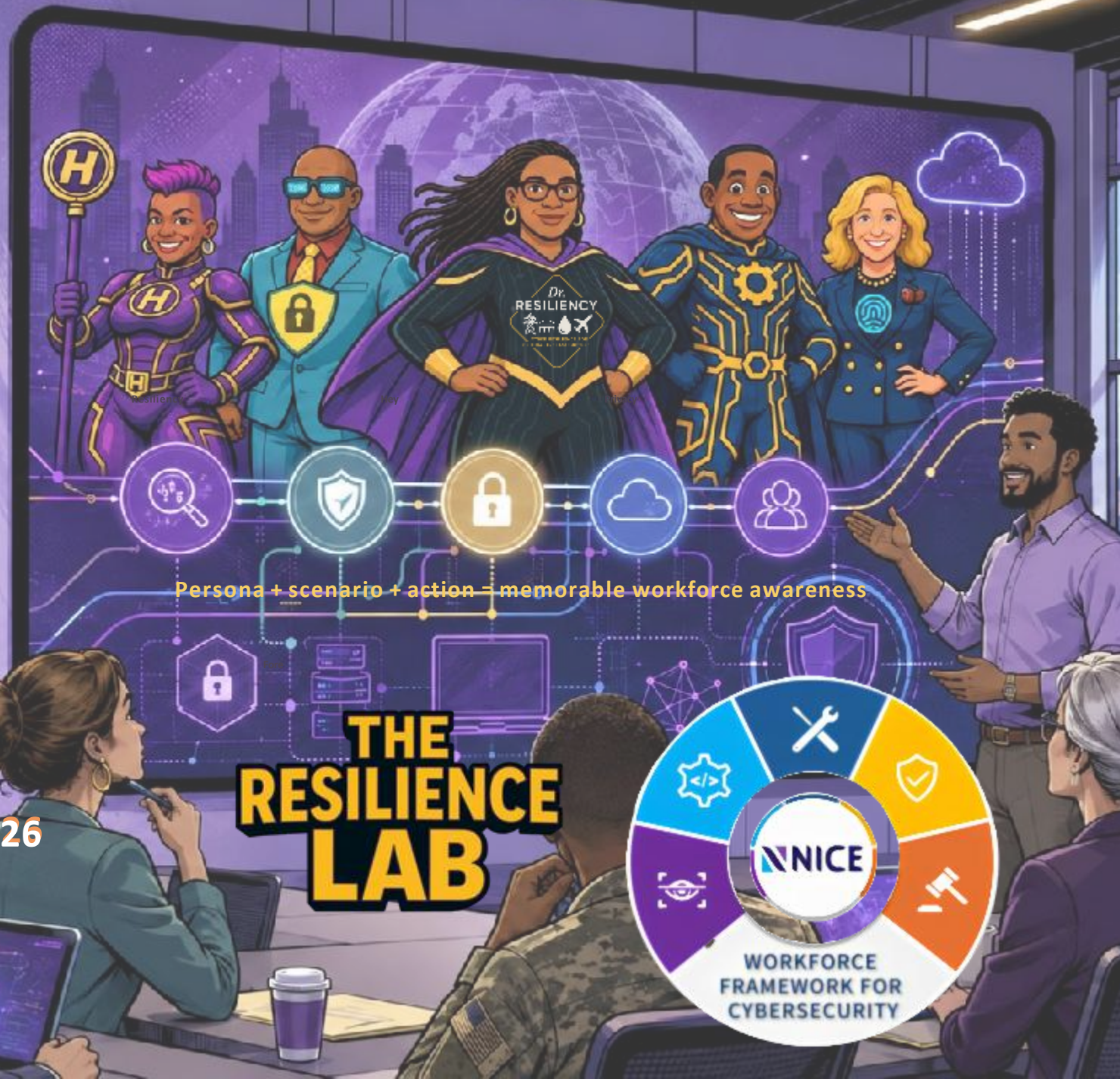
From Awareness to Action

Using storytelling, personas,
and comic characters to bring
the NICE Framework to life for
the current workforce.



FISSEA Fall Forum • September 15, 2026

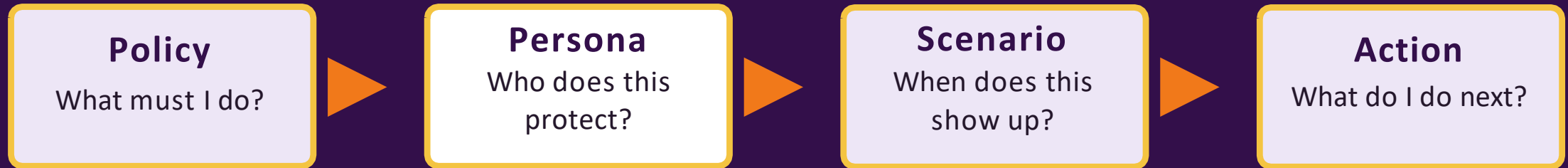
Dr. Natalie Foster Johnson
CyberMINDS Research Institute
Creator, The Resilience Lab



The Big Shift Needed



How do we make cybersecurity roles and responsibilities
memorable enough to influence behavior?
When awareness becomes a journey, not a single message.



From “training people on rules” to “placing people inside a cybersecurity story.”

Meet The Resilience Lab

The Resilience Lab for current workforce awareness

- | | |
|-----------------------------|--|
| FISSEA AUDIENCE | Federal awareness and training leaders need reusable tools, techniques, and resources for employee programs. |
| WORKFORCE GOAL | Move from “completed training” to “employees recognize their role when something happens.” |
| RESILIENCE LAB VALUE | A repeatable story pattern: character + scenario + behavior + reinforcement. |



Dr. Honey
Oversight and
Governance (OG)

Dr. Privacy
Privacy and
Defense (PD)



Dr. Resiliency
Implementation and
Operations (IO)

Dr. Know
Investigation (IN)

Dr. Forge
Design and
Development (DD)



The Awareness Challenge - Why the NICE Framework Belongs in Awareness?

NICE gives us a common language; storytelling helps it stick. Frame the problem facing awareness professionals:

NICE Framework
Work Role Categories
Work Roles
Competency Areas
Tasks, Knowledge & Skills



Role clarity

“Who owns what?” in plain language

Behavior clarity

“What action should I take?”

Mission clarity

“How does this protect the agency?”

NICE is the structure. Story is the delivery system.



- Employees are exposed to cybersecurity messages constantly.
- Annual training can become compliance-driven rather than behavior-driven.
- Technical terminology can make cybersecurity feel like “someone else’s job.”
- Employees may know the rule without understanding the consequence.

What if we gave cybersecurity responsibilities a face, personality, and story?

The Resilience Lab Character Roster

The Resilience Lab uses characters, visual storytelling, scenarios, and role-based learning to translate cybersecurity concepts into memorable experiences.



Dr. Resiliency

Risk, strategy,
resilience



Dr. Honey

Governance and
alignment



Dr. Forge

Secure design and
development



Dr. Privacy

Privacy and data
protection



Dr. Knows

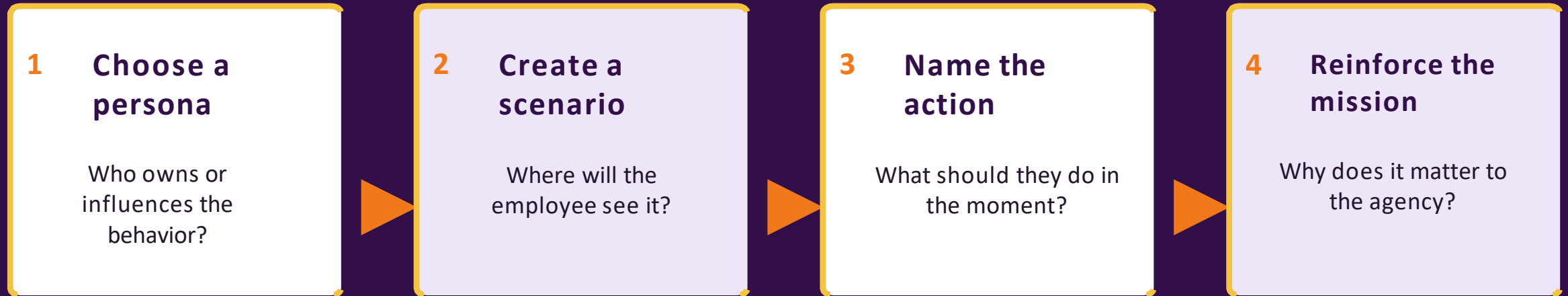
Training and
knowledge
sharing

**Use characters as communication anchors: one persona,
one behavior, one memorable scenario at a time.**

Core takeaway:

The characters are not the lesson. They are the vehicle for the lesson.

A Reusable Awareness Design Pattern



Youth education → Career exploration → Workforce awareness → Organizational resilience

The result: a micro-training module that can become a poster, email, video short, tabletop prompt, or manager huddle that is memorable and fun.

Storytelling works with adults because personas can simplify complex responsibilities without oversimplifying the risk.



Example Micro-Campaign - The Scenario

An employee receives an email that appears to come from agency leadership:

- **URGENT: “The Urgent Request”**

I'm heading into a meeting and need access to the sensitive project document in the cloud.

Please use the link below to update the sharing permissions and send me confirmation ASAP.

The sender's name looks familiar. The request sounds important. The employee feels pressure to act.

This is where the Resilience Lab team enters the story.

Dr. Knows — KNOW THE SIGNS

“What do we know about this message?”

Dr. Knows helps the employee recognize the clues:

- Unexpected request
- Sense of urgency
- Authority being used to create pressure
- Request involving sensitive information
- Request to change access permissions

Lesson: Recognize when something deserves a second look.

Employee action: STOP.

Dr. Honey — VERIFY THE REQUEST

“Don’t let a convincing story become a successful attack.”

Dr. Honey focuses on the human side of the attack.

The attacker is using **trust + authority + urgency** to influence the employee’s behavior.

Instead of replying to the suspicious email, the employee should verify the request through an **independent, approved channel**—such as a known internal number or established agency communication method.

Lesson: Trust—but independently verify.

Employee action: VERIFY.

Example Micro-Campaign - The Scenario - continued

Dr. Privacy — PROTECT THE INFORMATION

“Before you share it, know what you’re protecting.”

Dr. Privacy asks:

What information is in the document?

Who is authorized to see it?

Would changing permissions create unnecessary exposure?

Even if the request appears legitimate, sensitive information shouldn’t be shared simply because someone creates urgency.

Lesson: Protect the information before changing access.

Employee action: PROTECT.

Dr. Resiliency — PROTECT THE MISSION

The employee verifies the request.

Agency leadership never sent the email.

Because the employee stopped, protected the information, and verified the request, unauthorized access was prevented.

Dr. Resiliency connects that individual decision to the larger mission:

“Cyber resilience begins with decisions made before an incident becomes a crisis.”

The employee then follows the agency’s established procedure for reporting the suspicious message.

Employee action: REPORT.

STOP → PROTECT → VERIFY → REPORT

Dr. Knows: Know the signs. | Dr. Privacy: Protect the information. | Dr. Honey: Verify the request. | Dr. Resiliency: Protect the mission.

Three Federal Workforce Use Cases

How awareness teams can apply the method without building a full comic universe.

1. Role-based awareness

Adapt personas for leaders, supervisors, acquisition, IT, privacy, and general users.

Tailor behavior without making every lesson technical.

2. Mission-based campaigns

Connect actions to mission outcomes: protect data, preserve trust, keep services available, and reduce disruption.

Each campaign gets a story, scenario, and action.

3. Microlearning library

Turn one story pattern into quick lessons, posters, huddles, tabletop cards, and debriefs.

Reuse across the year.

SEE IT → UNDERSTAND IT → PRACTICE IT → REMEMBER IT → ACT



A 30–60–90 Day Implementation Playbook: From Awareness to Resilience

Start small. Build repeatable assets. Measure behavior, not just completion.

30 Days — Map

Pick 3 priority behaviors.
Map each to a persona,
scenario, and NICE-aligned
role or competency.

60 Days — Build

Create a starter kit: one
email, one huddle prompt,
one micro-lesson, and one
reinforcement message.

90 Days — Measure

Track reporting,
engagement, manager
participation, confidence,
and feedback. Iterate the
next campaign.

**Practical success measure: employees can explain the scenario,
identify the action, and know where to go next. The methodology is the KEY.**

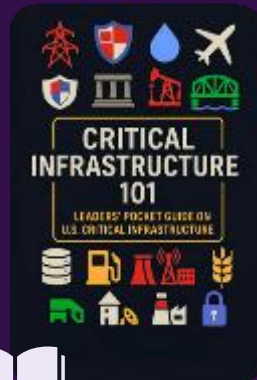
Organizations can create:

Department personas | Mission-based characters | Role archetypes
Scenario guides | Simple illustrated avatars | Recurring campaign voices

**The essential ingredients are consistency, recognizable roles, relevant scenarios, and actionable behaviors.
That makes the concept realistic for federal agencies with different budgets and resources.**

Closing Thought

Cybersecurity awareness works best when people can see themselves in the mission. The **NIST NICE Framework** gives us a shared language. Storytelling gives us the human connection. Awareness is not just about delivering information. It is about helping people understand where they fit into **cyber resilience**.



CYBERMinds



Thank you!

Dr. Natalie Foster Johnson
CyberMINDS Research Institute
njohnson@cybermindsinstitute.org



Q&A

Are There Any Questions?

Closing Remarks

Joyce Mui

FISSEA Co-Chair, Senior Manager Research Informatics,
University of Maryland Medical System & University of
Maryland Institute for Health Computing



THANK YOU

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

https://survey.nist.gov/jfe/form/SV_8hTFaMXOC9SHF2u

#FISSEA | nist.gov/fissea

Get Involved



Subscribe to the FISSEA Mailing List
FISSEAUUpdates+subscribe@list.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) Winter Forum**

February 9, 2027

#FISSEA | nist.gov/fissea