Federal Information Security Educators (FISSEA)

Fall Forum

September 17, 2024

1:00pm – 4:15pm ET

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Please Note…

This webinar and the engagement tools will be recorded.

An archive will be available on the event website.

Welcome and Opening Remarks

Marian Merritt
Deputy Director of NICE/FISSEA Lead
National Institute of Standards and Technology

Brooke Crisp
FISSEA Co-Chair

Get Involved

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

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

Cyber Esports: Training High Performing Teams

Jessica Gulick
CEO & Founder
Katzcy and PlayCyber

GET IN THE GAME.

Cyber Esports: Training High Performing Teams

Jessica Gulick

Founder, PlayCyber

Commissioner, US Cyber Team

PLAY CYBER

PlayCyber CEO

JESSICA GULICK

CYBER MARKET EXPERT, CYBERSECURITY EXPERT, CYBER ESPORT VISIONARY. COMMUNITY AND MARKETING GURU, CISSP, MBA

- Founded PlayCyber 2019 - today engages over 8K players across 50+ countries annually, includes global cyber leagues, Wicked6, US Cyber Games, Global Cyber Games, Charity Cyber Battle and more
- Commissioned 1st ever US Cyber Team and Women's Team
- Founded Katzcy in 2015 - today operates $1M+ in annual business, provides growth consulting to cyber firms
- Captured $2.5B in opportunities as an expert cyber team of 34
- Directed the first Maryland Cyber Conference & Challenge
- Co-authored a number of NIST Special Publications
- MBA from Virginia Tech

MISSION:

CREATE A GLOBAL CYBER ESPORT

ADVANCING THE CYBER WORKFORCE

CYBER GAMES | COMPETITIONS | ESPORTS | EVENTS | MARKETING

Katzcy is a community of brands that promotes, supports, and advocates for cybersecurity workforce growth and diversification

High-Performing Teams Makes the Impossible Possible

Competition Drives Proficiencies

Advancing the Cyber Workforce Protects Our Future

Diversity and Inclusion Creates a Competitive Advantage

Passion Drives Positive Change

Collaboration is Key to Making an Impact

THE POWER OF SPORTS

- **Delivers an engaging and immersive learning experience**
- **Fosters mental resilience and endurance**
- **Instills teamwork and leadership skills in high-pressure scenarios**
- **Offers a secure environment to experiment and gain insights into the mechanics of an attack**
- **Enhances confidence and skill development**

Interestingly, 94% of women executives in C-suite positions have a background in sports.

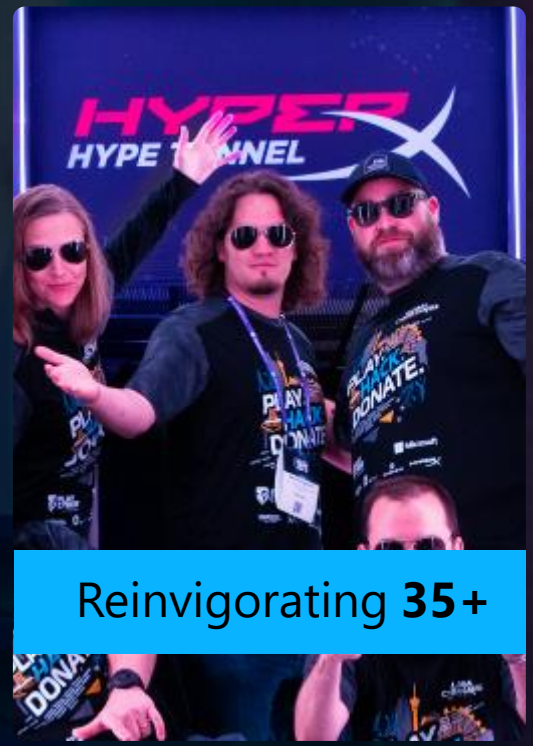
GET IN THE GAME.

A LIFELONG ♥ FOR THE GAMES

Inspiring **K-12**

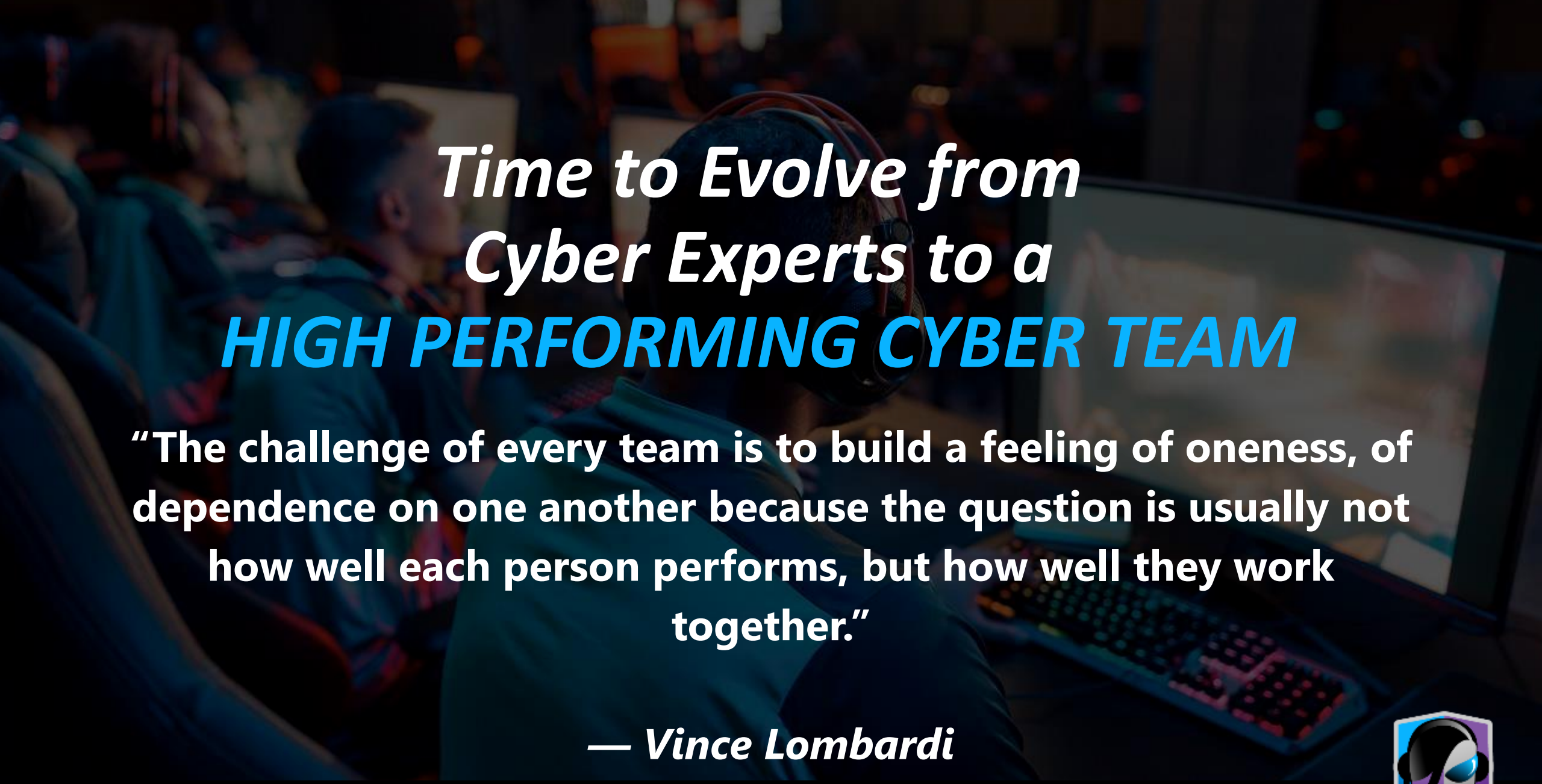
Igniting **18-25**

Sharpening **25 -35**



Reinvigorating **35+**

GET IN THE GAME.



Time to Evolve from Cyber Experts to a HIGH PERFORMING CYBER TEAM

"The challenge of every team is to build a feeling of oneness, of dependence on one another because the question is usually not how well each person performs, but how well they work together."

— Vince Lombardi

GET IN THE GAME.

High Performing Cyber Teams

- **HPC Teams practice:**
  - **Role delineation**
  - **“Loving your passes”**
  - **Prioritization “Triage”**
  - **Understanding the Goal**
  - **Seeing the Game board**
  - **Knowing Teammate’s Strengths and Communication Styles**
  - **Building human redundancies**
  - **Staying healthy (Physical and Mental)**
  - **Detailed plays**
  - **Practice, Hot wash, Refine, Practice**
  - **Play together**

GET IN THE GAME.

It takes more than just technical skills.

GET IN THE GAME.

KEY PERFORMANCE ATTRIBUTES

Similarities: practices, infrastructures, resources and talent sources.
We can take best practices honed over **decades of research and experience** and apply it to innovate in cybersecurity talent and workforce development.

SPORTS
Performance Attributes

- Strength
- Speed
- Condition/Energy
- Positioning/Mobility

ESPORTS
PERFORMANCE ATTRIBUTES

- Dexterity
- Speed
- Condition/Endurance
- Game Map Awareness

CYBER ESPORTS
Performance Attributes

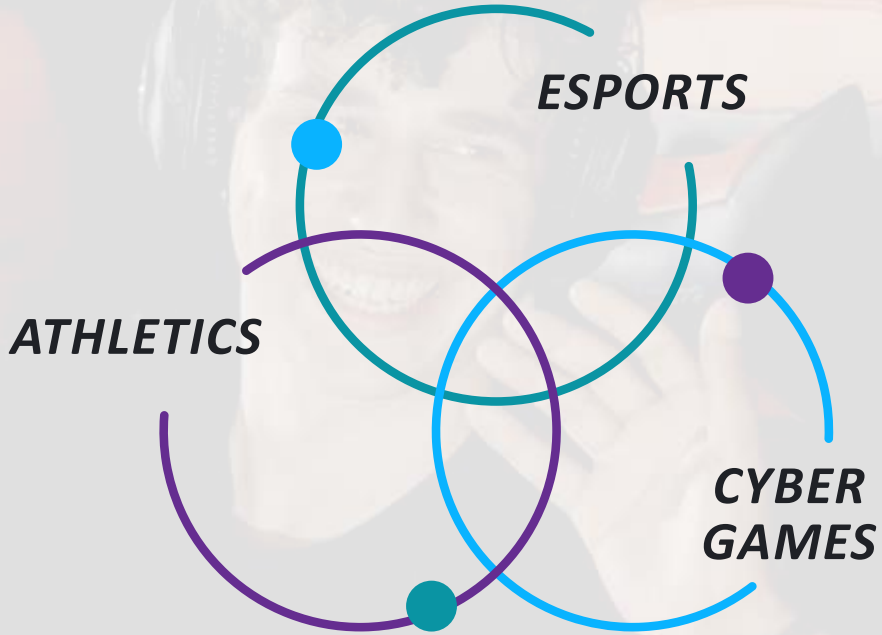
- Cognitive/Smarts
- Speed
- Condition/Focus
- Positioning/Skill Range

SHARE CORE SKILLS

- Teamwork and collaboration
- Time management and organizational skills
- Critical Thinking and creative problem solving
- Perseverance and Adaptive Learning

GET IN THE GAME.

MOVING FROM SMART PLAYERS TO A HIGH-PERFORMING CYBER TEAM



ATTRIBUTES

- Cognitive Endurance
- Game Board Awareness
- Speed & Proficiency
- Multi-Skill Range
- Identify, Analyze and Solve

CORE SKILLS

- Coaching and Mentorship
- Competitive Drive
- Teamwork and Collaboration
- Time Management and Organizational Skills
- Critical Thinking and Creative Problem Solving

KNOWLEDGE

- Cryptography
- Digital Forensics
- Binary Exploitation
- Reverse Engineering
- Web Security
- Vulnerability Research
- Tool Developing
- Networking/Architecture

GET IN THE GAME.

WHAT WOULD CYBER ROLES BE

Football	League of Legends	Example Cyber Team
Quarterback	Top Laner	Hunters (finds vulns)
Wide Receiver	Mid Laner	Fighters (exploits)
Defensive Back	Junglar	Lead/Support / Triage
Safety	AD Carry	Orchestrators (auto/tools)
Kicker	Support	Meisters (Crypto, RE, etc)

GET IN THE GAME.

PUTTING IT TO WORK

Build Your Resume

Add to Annual Review

Submit as Training

Team Outings

Submit for CPUs

Track Your Progress

GET IN THE GAME.

TIPS IN GETTING STARTED

- Expand your network - connect with 2-3 people to collaborate with
- Create your environment - familiarize yourself with platforms like Discord, GitHub, VMs, etc.
- Develop your strategy -
  - Start with your strengths (topic)
  - Experiment within sandboxes
  - Focus on progress rather than winning at first
  - Establish a schedule to avoid feeling overwhelmed
- Monitor your activities and progress (align with the NICE framework and job skills)
- Remember, not all games are the same; stay adaptable
- Take the plunge - Get in the Game!

WHERE TO PLAY

US CYBER GAMES

PLAY CYBER

WICKED 6 CYBER GAMES

CTF TIME

Check out this site for a list of games in the next two weeks.

MetaCTF

NCL

SANS CYBER RANGES

HACKTHEBOX

Try Hack Me

picoCTF

GET IN THE GAME.

Cybersecurity and Infrastructure Security Agency's President's Cup Cybersecurity Competition

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

- CISA's annual CTF competition open to the entire federal workforce including uniformed service members.
- Three rounds over 3-4 months concluding with Finals in CISA facilities.
- Participants can compete as an Individual and/or on a Team of up to five members.
- All challenges made available on the Practice Area and CISA GitHub repo.
- Visit cisa.gov/presidentscup or contact presidentscup@cisa.dhs.gov to learn more!

US CYBER GAMES

IGNITE YOUR CYBER CAREER

A week-long cyber career event!

MONDAY, SEPT. 23 – FRIDAY, SEPT. 27

SECURE YOUR VIRTUAL SEAT ▶

THE WORLD NEEDS MORE WOMEN IN CYBER

WICKED6 CYBER GAMES

2024 WOMEN'S GLOBAL CYBER LEAGUE

CYBER ESPORTS DRIVES DIVERSITY

- Low cost to entry
- Team sport
- Flexible Schedules
- Skills-based success
- Hands-on learning as a group
- Watch to play
- No heels required

Learn more: **www.wicked6.com**

Q&A

Are There Any Questions?

Beyond Compliance: Where Digital Badges Work Better

Daniel T. Hickey
Professor and Program Coordinator
Indiana University

Beyond Compliance:
Where Digital Badges Work Better

Daniel T. Hickey
Professor and Program Coordinator
Learning Sciences Program
Indiana University

Presentation at the Fall Forum of the Federal Information Security Educators (FISSEA), September 17, 2024

INDIANA UNIVERSITY

A PERVASIVE TECHNOLOGY INSTITUTE RESEARCH CENTER

Center for Applied Cybersecurity Research

Member of the IU Cybersecurity Community

CRLT

Center for Research on Learning & Technology

Indiana University | School of Education

Building the Field of
Digital Media and Learning

MacArthur
The John D. and Catherine T. MacArthur Foundation

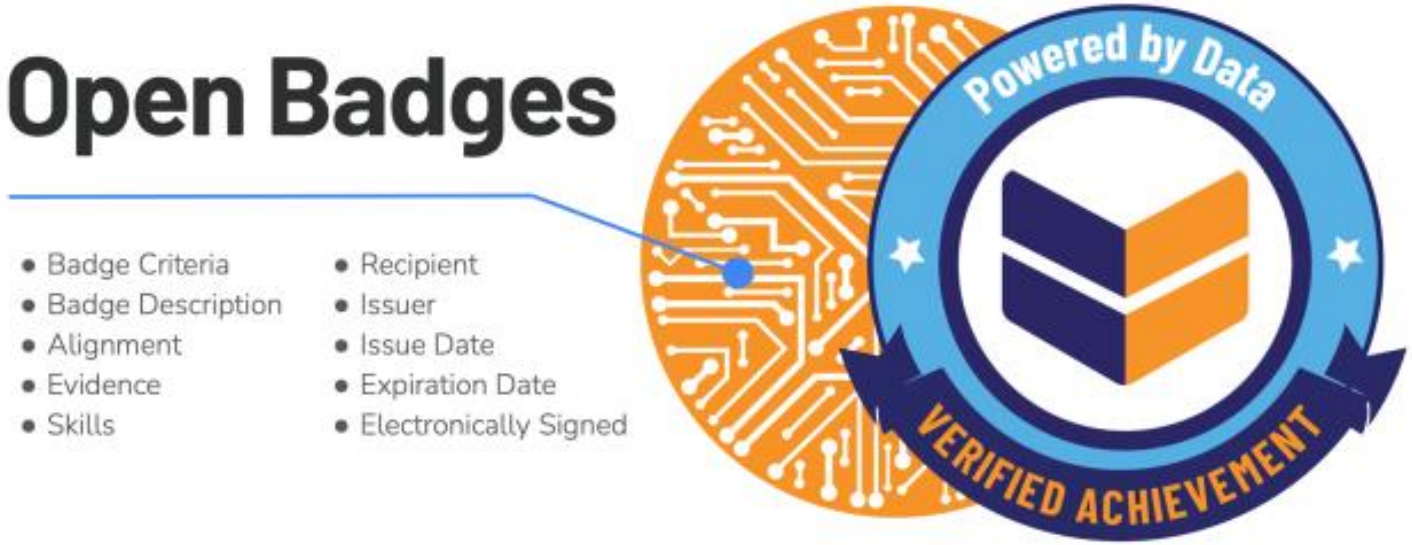
National Science Foundation
Directorate for Education and Human Resources (EHR)


DIGITAL
MEDIA+
LEARNING
competition 4
BADGES FOR LIFELONG LEARNING
HASTAC
INITIATIVE
COLLABORATING
WITH
mozilla
SUPPORTED BY
MacArthur
Foundation


DIGITAL
MEDIA+
LEARNING
competition 4
SUPPORTED BY
MacArthur
Foundation

DIGITAL BADGES CONTAIN INFO
Claims & evidence; links to more

- Contain specific claims and detailed evidence supporting claims
- This is different from conventional credential
- Can link to unlimited additional information

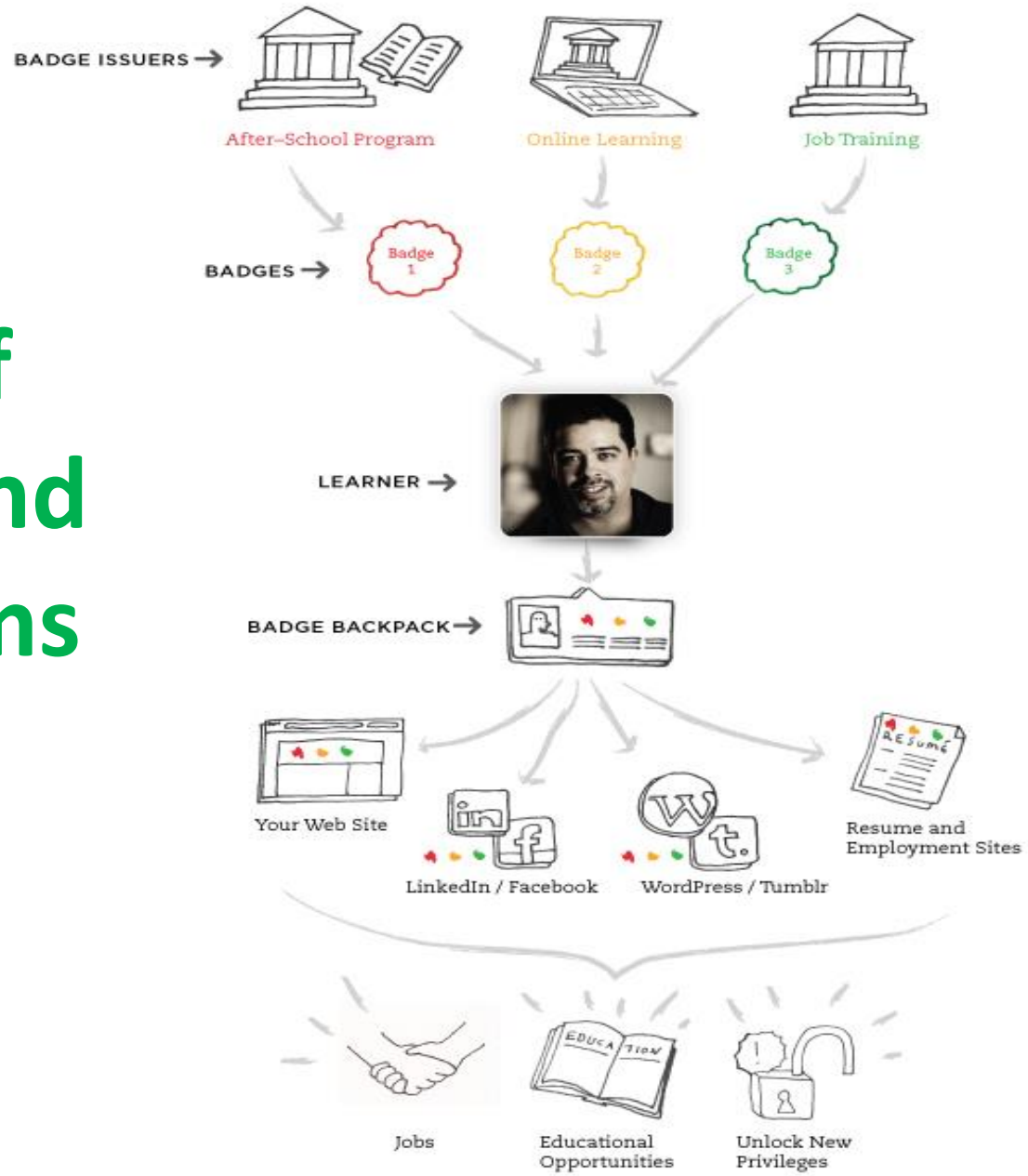


OPEN BADGES CIRCULATE

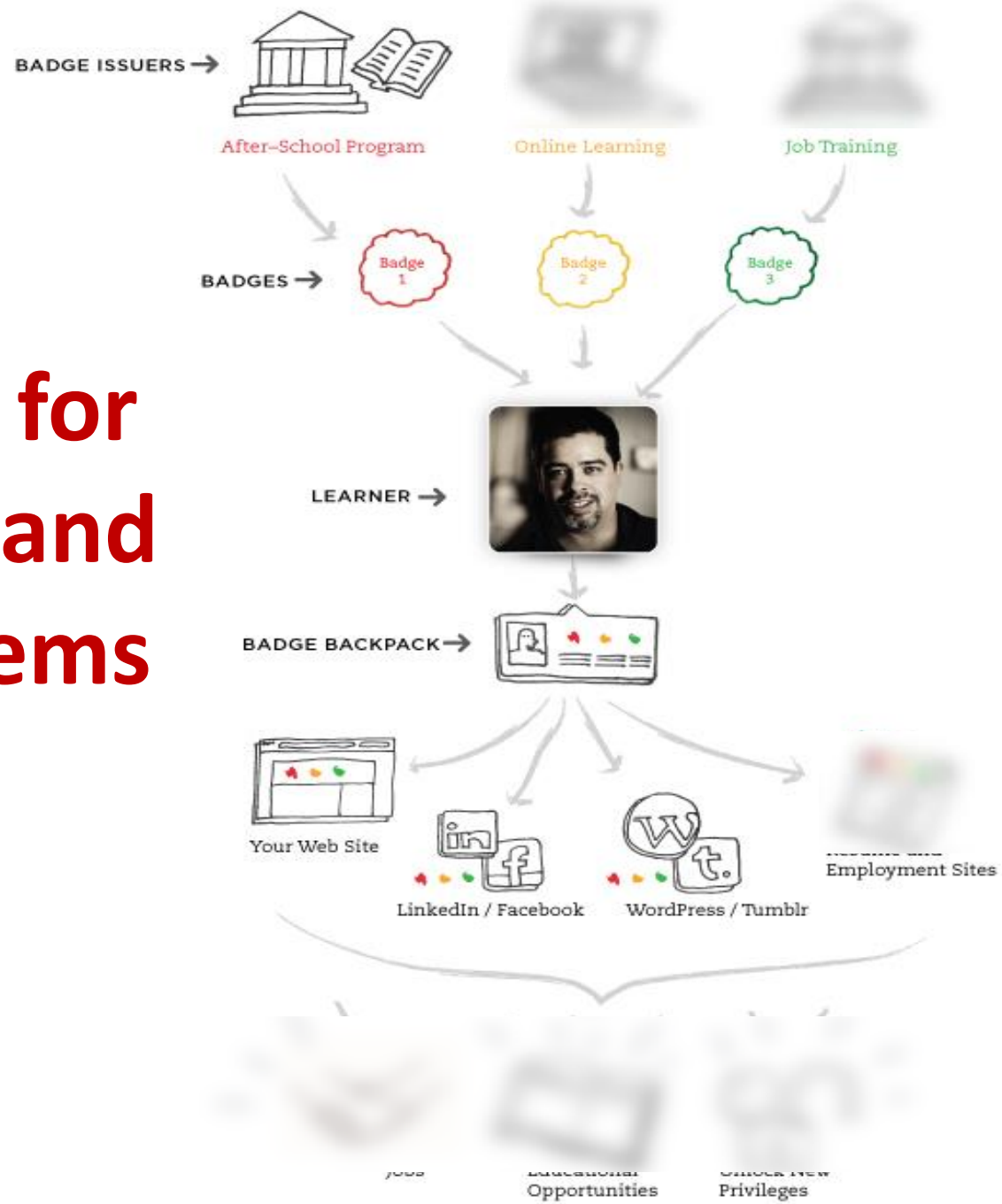
Info circulates in valued networks

- Credibility of claims and validity of evidence gets "crowdsourced"
- Earners can find opportunities and promote achievements
- Institutions can recognize broader accomplishments
- Employers can communicate needs and find skills
- **The goal is creating "badge-based learning ecosystems"**

The Promise of Digital Badges and Badge Ecosystems



The Challenge for Digital Badges and Badge Ecosystems



NEWS

How Open E-Credentials Will Transform Higher Education

By Daniel T. Hickey | APRIL 9, 2017

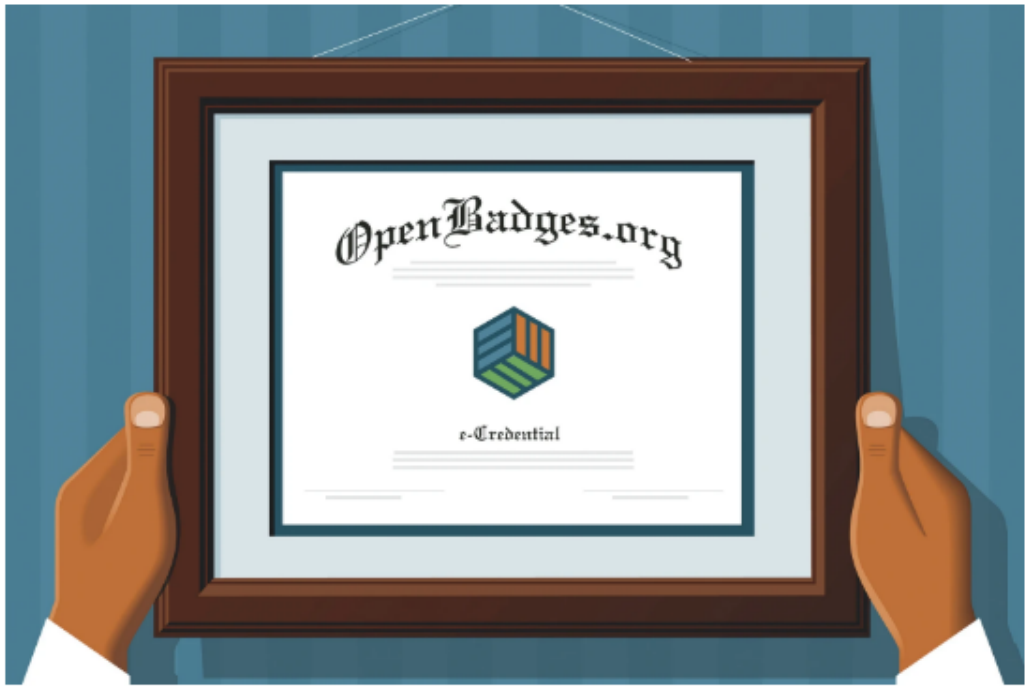


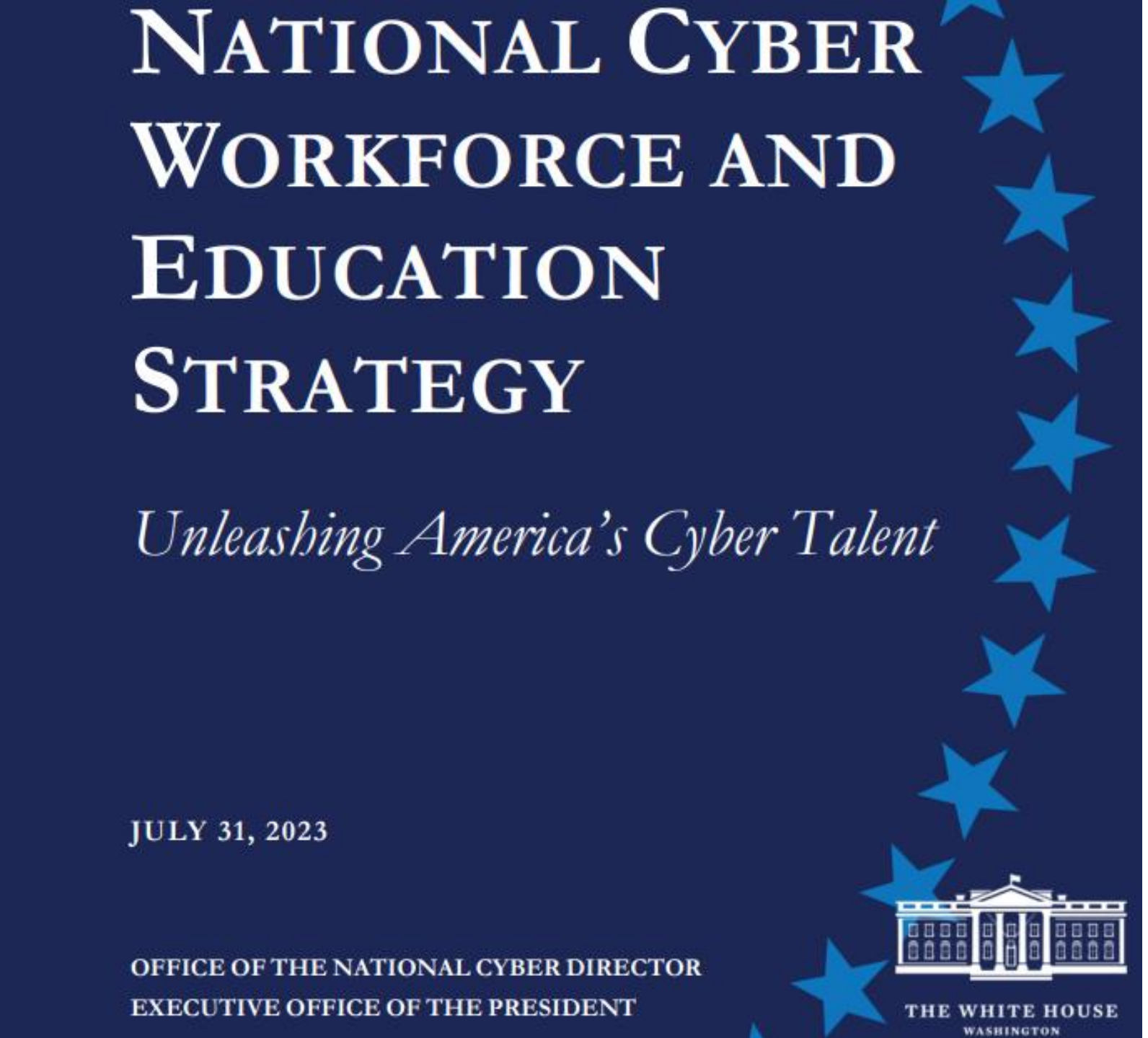
ILLUSTRATION BY JOHN W. TOMAC FOR THE CHRONICLE

Those who dismiss higher-education e-credentials today are acting like retailers who dismissed e-commerce 20 years ago.

Those who dismiss higher-education e-credentials today are acting like retailers who dismissed e-commerce 20 years ago.

At that time, many retailers, publishers, and booksellers were skeptical of consumer e-commerce. Amazon's 1997 claim to be the "Earth's biggest bookstore" garnered lots of attention, as did Barnes & Noble's lawsuit claiming that Amazon should not be allowed to call itself a real bookstore. While the standards for web payments were well established by 1997, it took perhaps another 10 years for consumer reviews to become sufficiently numerous and credible to create the trust networks that would allow consumer e-commerce to become a thriving and sustainable business model. But by that time, some vendors who were slow to embrace e-commerce had already begun their slow but steady slide toward closures, layoffs, and bankruptcies.

Those who dismiss higher-education e-credentials today are acting like retailers who dismissed e-commerce 20 years ago.



- Pillars:
  - Equip every American with foundational cyber skills.
  - Transform cyber education.
  - Expand and enhance America's cyber workforce.
  - Strengthen the federal cyber workforce.

NATIONAL CYBER WORKFORCE AND EDUCATION STRATEGY

Unleashing America's Cyber Talent

How Badges Might Support Pillar One: *Equip Every American with Foundational Cyber Skills*

NCWCG Lines of Effort	Potential Badge Roles
1.1.2 Foster ecosystem approaches to enhance foundational cyber skill learning opportunities.	**The whole point is creating "badge-based learning ecosystems"**
1.1.3 Encourage the development of an open knowledge network for foundational cyber skills	Badges are ideal for recognizing learning in such networks
1.1.5 Include foundational cyber skills in existing educational frameworks, programs, and activities.	Badges are ideal for introducing new content to existing programs
1.2.3 Leverage national outreach and awareness initiatives to encourage the development of foundational skills and the pursuit of careers.	Shared badges in social networks are ideal for helping others find learning opportunities

NATIONAL CYBER WORKFORCE AND EDUCATION STRATEGY

Unleashing America's Cyber Talent

How Badges Might Support Pillar Two: *Transform Cyber Education*

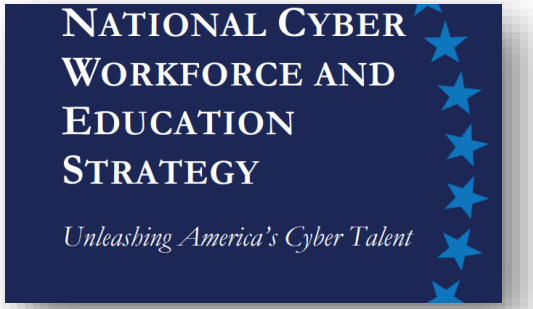
NCWCG Lines of Effort	Potential Badge Roles
2.1.1 Expand and support cyber education ecosystems.	Again, badge are intended to support learning ecosystems
2.1.2 Increase engagement in cyber education ecosystems.	Motivating engagement is a core function of digital badges
2.1.3 Integrate cybersecurity across disciplines to prepare the cyber workforce to build systems that are secure by design.	**Badges are "boundary objects" that maintain meaning across disciplinary boundaries**
2.2.4 Increase concurrent and transferrable credit opportunities.	Badges are central to some new dual-enrollment and credit transfer schemes

NATIONAL CYBER WORKFORCE AND EDUCATION STRATEGY

Unleashing America's Cyber Talent

How Badges Might Support Pillar Two: *Transform Cyber Education*

NCWCG Lines of Effort	Potential Badge Roles
2.2.5 Expand innovative models for academic credit (i.e., competency-based education)	**Badges are prominent in CBE and learning and employment records**
2.3.5 Encourage interdisciplinary approaches to teaching cyber.	Motivating engagement is a core function of digital badges
2.3.6 Incorporate cyber education and training into career pathway initiatives.	Most badging systems (e..g., *Canvas Badges*) include pathways
2.3.7 Expand opportunities to earn credits for experiential learning in cyber.	Badges are ideal for recognizing experiential learning

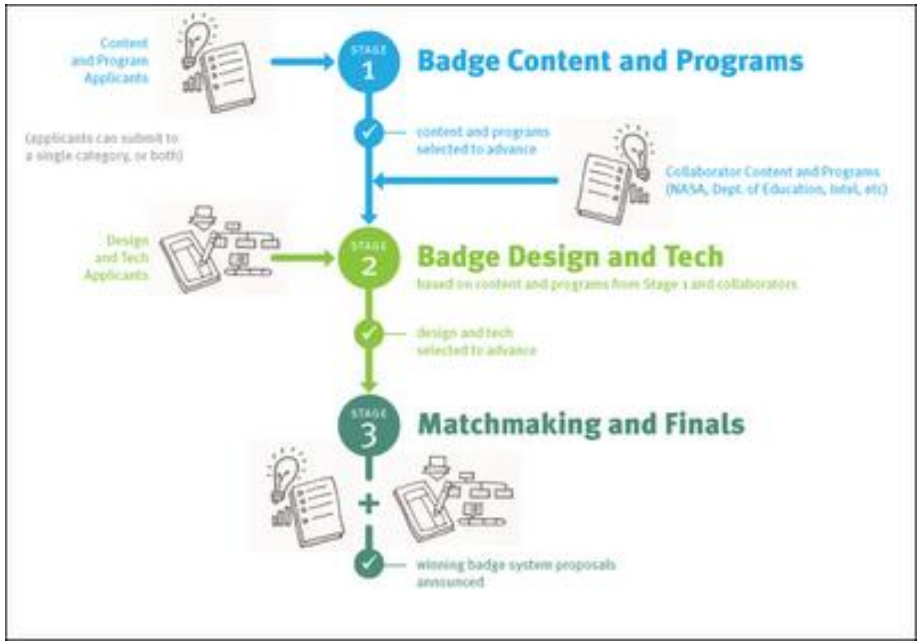


How Badges Might Support Pillar Three: *Expand and Enhance America's Cyber Workforce*

NCWCG Lines of Effort	Potential Badge Roles
3.1.3 Expand the availability of low- or no-cost workforce development tools for small enterprises.	Badges are ideal for inexpensive open learning networks
3.2.3 Expand the use of skills-based hiring practices **3.2.4 Expand the use of skills-based workforce development practices.**	**Badges epitomize skills-based hiring and development**
3.2.5 Increase on-ramps to cyber careers through work-based learning opportunities.	Badges are well-suited for work-based learning

Lessons Learned from the *Badges for Lifelong Learning* Initiative in the *Design Principles Documentation* Project (2012-2016)

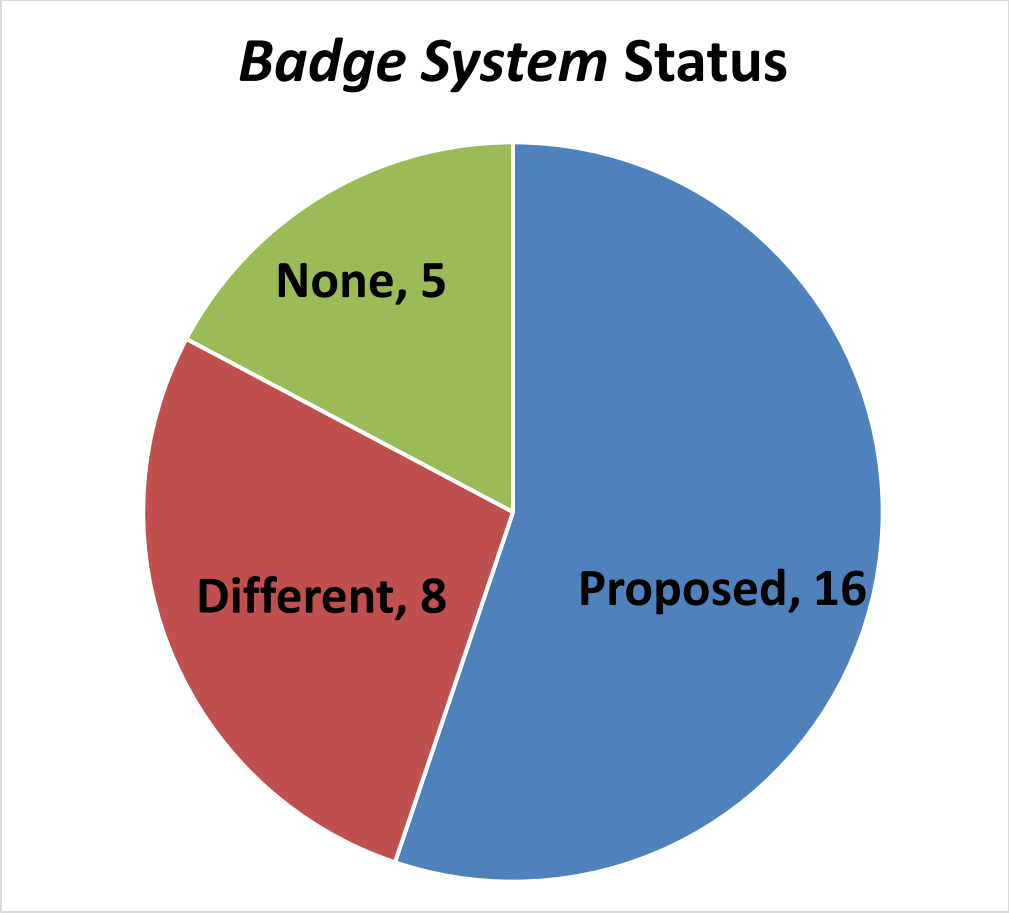
The Design Principles Documentation Project

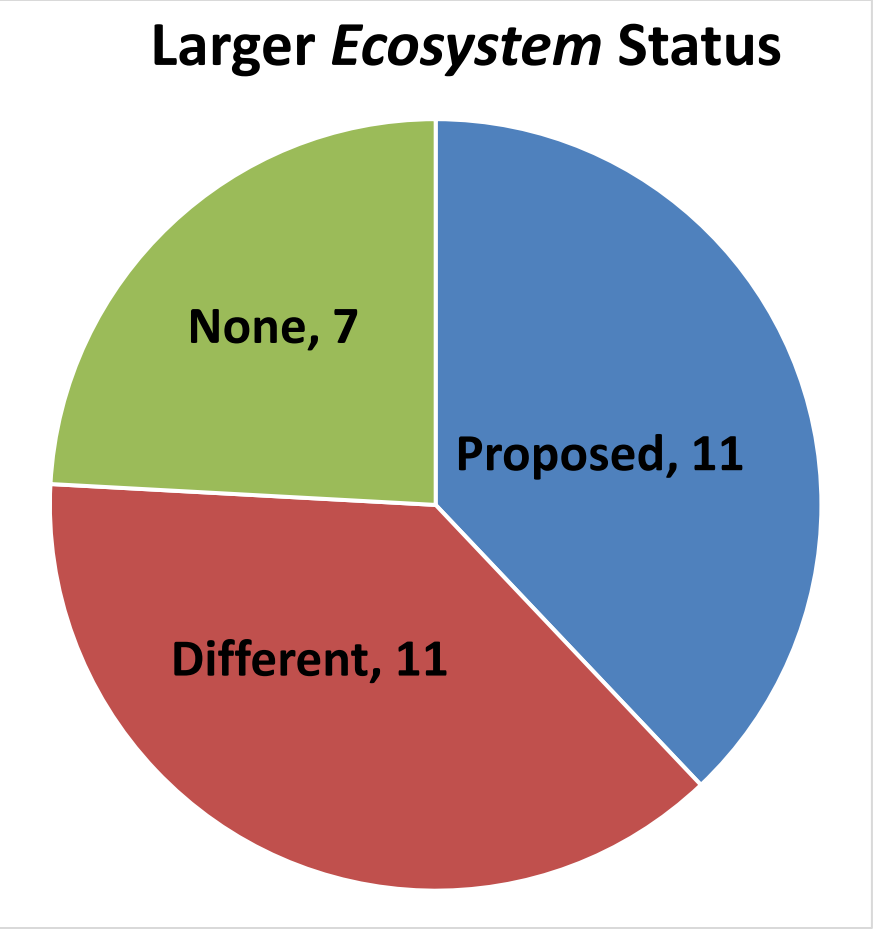


- Studied 2012 DML content awardees
- 600 badge content proposals
- 29 content developers supported
- 3 platforms supported


youtopia
HASTAC
Humanities, Arts, Science, and Technology Advanced Collaboratory
pragmatic
without us, it's just a game™
Badge Stack
P2PU
PROJECT WHITECARD
gogo LABS
shake-it-up learning
3D GAME LAB
Social Impact Exchange
Taking successful innovation to scale
intel
INTERNATIONAL SCIENCE AND ENGINEERING FAIR
Girl Scouts®
SOCIETY FOR SCIENCE & THE PUBLIC
Inform. Educate. Inspire.
MANUFACTURING Institute
makewaves
StoryCorps
The conversation of a lifetime
ROADTRIP NATION
Define your own road in life.
Microsoft Partners in Learning
PASA
PROVIDENCE AFTER SCHOOL ALLIANCE
buzz Math
EARTHWORKS
HIVE
Digital Media Learning Fund
in The New York Community Trust
BADGES FOR VETS
yalsa
Young Adult Library Services Association
NOAA
ASI
asi.ucdavis.edu
SWEET WATER FOUNDATION
There grows the neighborhood
ASHP·CML
EffectiveSC
ES2N
computer science student network
DFA
DESIGN for AMERICA
COOPER-HEWITT
NATIONAL DESIGN WEEK
MASTER HISTORY TEACHER
CENTER FOR EDUCATIONAL TECHNOLOGIES
Smithsonian
National Museum of Natural History

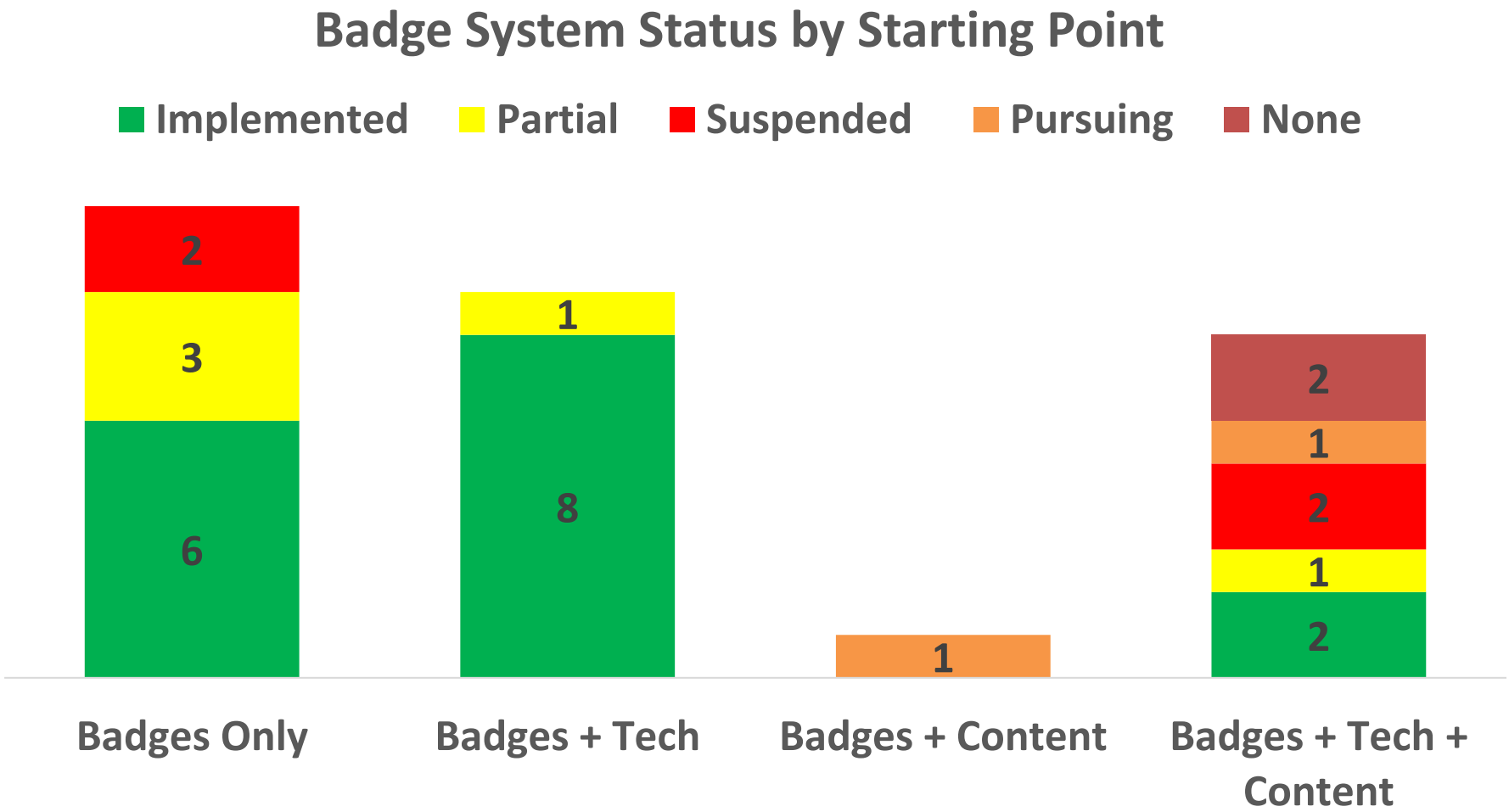
Badges Work Better….
In Some Places than Others





Badges Work Better….

Where Content and Tech Already Exist



Build Less ⟷ Build More

Badges Work Better….
As Informal Credentials

- The most obvious value practices (formal credit) were hardest to enact
  - 1 out of 5 (*PASA*) succeeded in awarding formal credit
  - *3D Game Labs* implemented most other practices
  - *Level Up, Youth Digital Filmmaker, SA&FS* suspended efforts

Badges Work Better….
When Internally Valued

- Six projects failed to gain external endorsement for various reasons
  - *Who Built America?* reported that the National Council for the Social Studies “did not really understand the concept of badges”.
  - *National Manufacturing Badge System* reported that the manufacturers “understood badges but did not trust their validity.”

Badges Work Better….
When They Offer Unique Information

- Redundant badge systems struggled
  - –The badges at 4-H duplicated existing credentials & network
  - –Eventually built a completely different system

Available soon via multiple devices...

Badges Work Better….
Where Learning is Social and Networked

- *S2R Medals* and *MOUSE Wins!*
  Excelled by finding other ways to add value
  - The learning was social and networked
  - Included some “participation” badges
  - Assessment was social and distributed
  - layered badges into existing content & tech

Badges Work Better….
Where Learning is Social and Networked

- More competency-based systems failed
  - *Level Up* and *SA&FS* could not shift from credit hours to competencies
  - *Pathways to Global Competence* never got off the ground
  - *Manufacturing Institute* employers would not endorse competency badges
  - YALSA scaled back multiple badges for specific competencies to a single completion badge

ABOUT THIS BLOG

New models of learning and new digital technologies require new approaches to assessment. We explore and discuss new approaches to assessment, with a particular focus on participatory approaches, digital badges, learning recognition networks, ePortfolios, and eCredentialing.

ABOUT THESE BLOGGERS

THURSDAY, MAY 13, 2021

Articles Chapters, and Reports about Open Badges

by Daniel Hickey

Thanks to Connie Yowell and Mimi Itow at the MacArthur Foundation's Digital Media and Learning Initiative, I had the pleasure of being deeply involved with digital badges and micro-credentials starting in 2010. While we no longer have any funding for this work, my colleagues and I are continuing to engage with the community. I am thrilled to see the continued growth and the wide recognition that micro-credentials offer new career pathways to non-traditional learners.

I get occasional requests for copies of chapters, articles, and reports that we reproduced as well as some general "where do we begin" queries. Given that we were funded to provide broad guidance from 2012-2017, we produced some things that beginners and advanced innovators have found quite useful. We continued to publish after MacArthur ended the DML initiative and funding ran out. Here is an annotated list of resources. We hope you find them useful!

Getting Started.

If you are new to badges and microcredentials, this might be a good place to get some basic background:

- Hickey, D. T. , (2017). *Badges*. In K. Peppler (Ed.) *Encyclopedia of out-of-school learning*: Volume 1 (pp. 460-463). Los Angeles, CA: Sage Publications.

Where Badges Work Better

RE-MEDIATING ASSESSMENT

WHEREIN WE CONSIDER THE POSSIBILITIES FOR PARTICIPATORY APPROACHES TO ASSESSMENT OF LEARNING WITH DIGITAL BADGES, ONLINE LEARNING, OPEN COURSES, MOOCS, AI, AND BEYOND

SEARCH THIS BLOG

Search

SUBSCRIBE

Posts

Comments

https://bit.ly/RMAbadges

ABOUT THIS BLOG

New models of learning and new digital technologies require new approaches to assessment. We explore and discuss new approaches to assessment, with a particular focus on participatory approaches, digital badges, learning recognition networks, ePortfolios, and eCredentialing.

ABOUT THESE BLOGGERS

THURSDAY, MAY 13, 2021

Articles Chapters, and Reports about Open Badges

by Daniel Hickey

in

credentials offer new career pathways to non-traditional learners.

I get occasional requests for copies of chapters, articles, and reports that we reproduced as well as some general "where do we begin" queries. Given that we were funded to provide broad guidance from 2012-2017, we produced some things that beginners and advanced innovators have found quite useful. We continued to publish after MacArthur ended the DML initiative and funding ran out. Here is an annotated list of resources. We hope you find them useful!

Getting Started.

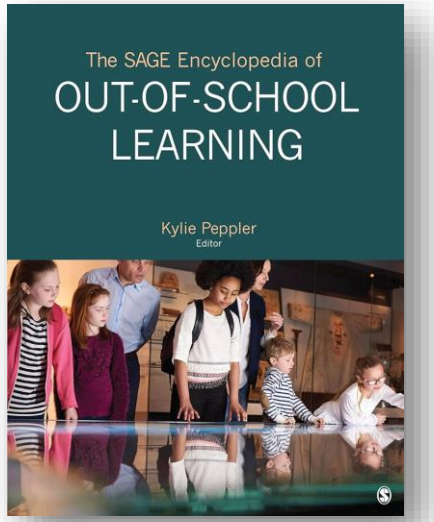
If you are new to badges and microcredentials, this might be a good place to get some basic background:

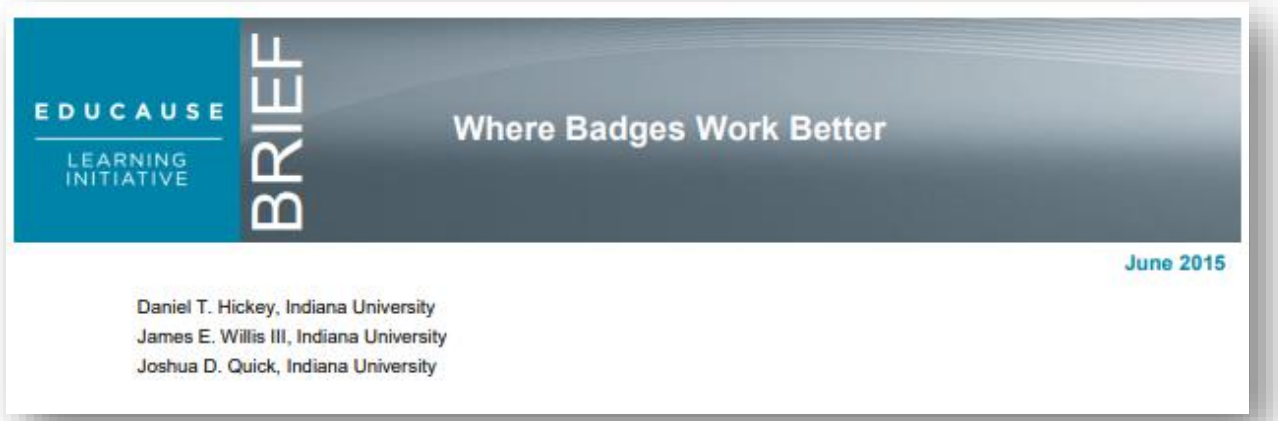
- Hickey, D. T. , (2017). *Badges*. In K. Peppler (Ed.) *Encyclopedia of out-of-school learning*: Volume 1 (pp. 460-463). Los Angeles, CA: Sage Publications.

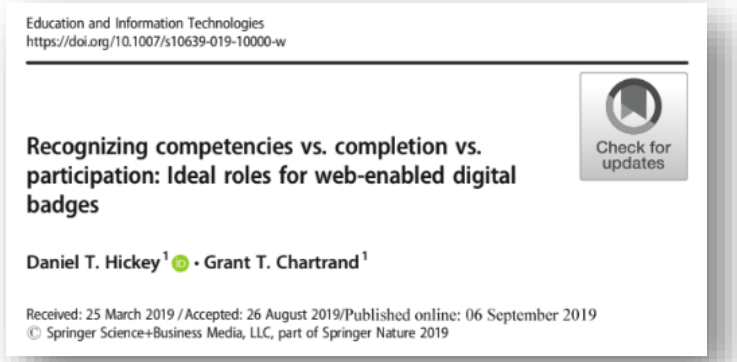
Where Badges Work Better

https://bit.ly/RMAbadges

“Where Badges Work Better”

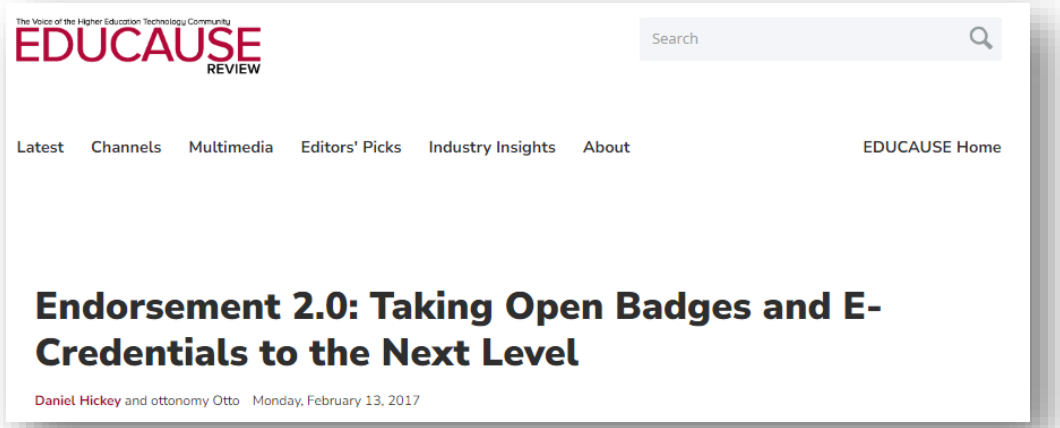


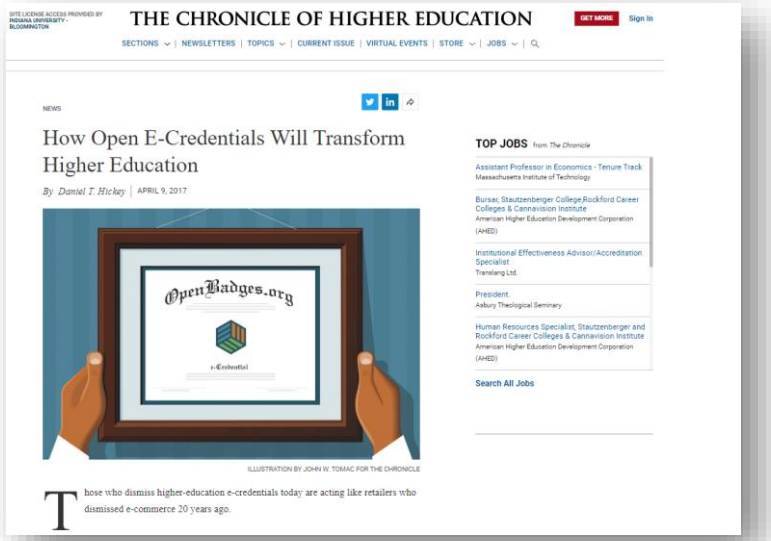


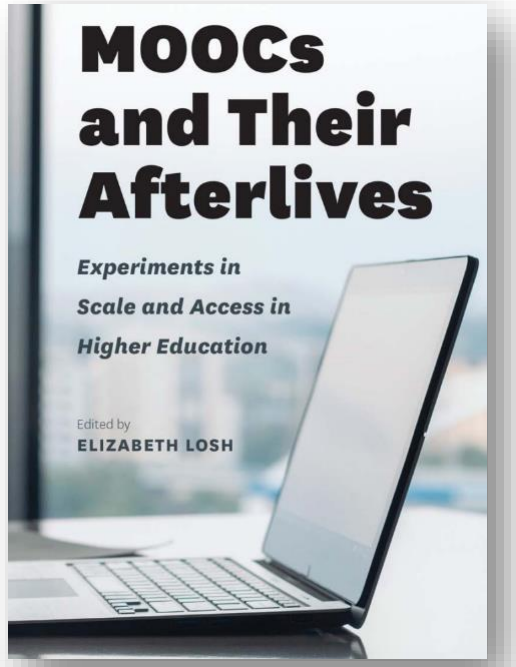


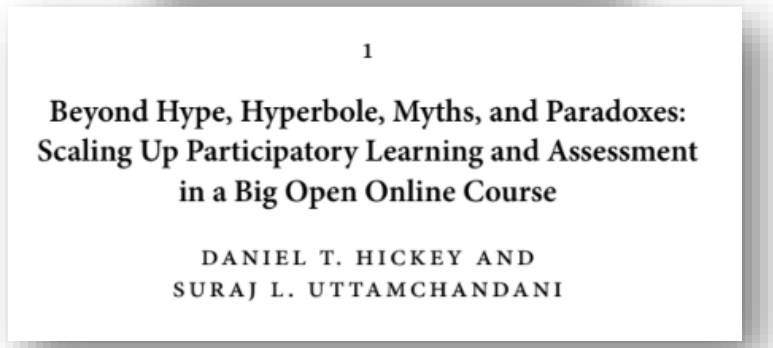
https://bit.ly/RMAbadges

“The Power of Endorsement”



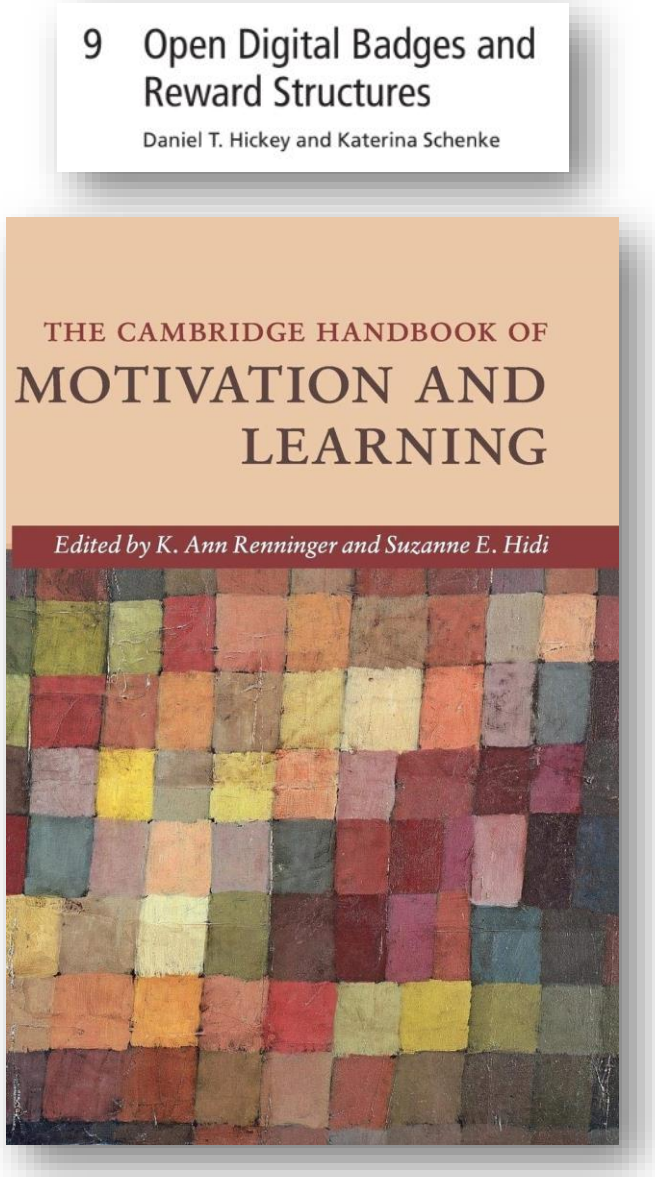






https://bit.ly/RMAbadges

“Motivating Learning with Badges”



- Seven Arguments about Motivating Learning with Digital Badges:
  - Digital badges are inherently meaningful.
  - Open digital badges are particularly meaningful.
  - Open badges are particularly consequential credentials.
  - The negative consequences of extrinsic rewards are overstated.
  - Focus primarily on social activity and secondarily on individual activity.
  - Situative models of engagement are ideal for studying digital credentials.
  - Study motivation and digital credentials at three “levels.”

https://bit.ly/RMAbadges "New Perspective on Validity"

THE INFORMATION SOCIETY
2016, VOL. 32, NO. 2, 117–129
http://dx.doi.org/10.1080/01972243.2016.1130500

Routledge
Taylor & Francis Group

Transcending conventional credentialing and assessment paradigms with information-rich digital badges

Carla Casilli[a] and Daniel Hickey[b]

[a]The Badge Alliance, Los Angeles, California, USA; [b]School of Education, Indiana University, Bloomington, Indiana, USA

ABSTRACT

Open digital badges are Web-enabled tokens of learning and accomplishment. They operate in an environment of explicit (rather than tacit) trust; open badges provide issuers the ability to include specific claims and associate those claims with detailed supporting evidence. Earners are encouraged to share their badges over social networks, e-mail, and websites, and the information they contain is expected to circulate readily in these spaces. Building upon current concepts and theories from the Information Sciences and Learning Sciences, this article shows how the informational affordances of digital badges are transforming education and learning more generally, and more particularly by transcending conventional paradigms of academic credentialing and educational assessment.

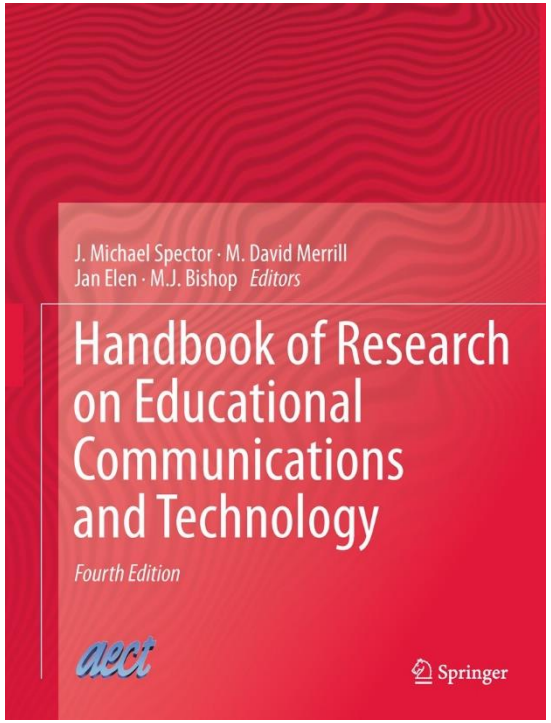
ARTICLE HISTORY
Received 1 May 2014
Accepted 23 March 2015

KEYWORDS
Assessment; connected learning; credentialing; digital badges; education; open badges; technology

https://bit.ly/RMAbadges "The Transformative Functions of Badges"

Competencies in Context: New Approaches to Capturing, Recognizing, and Endorsing Learning

Daniel T. Hickey, Suraj L. Uttamchandani, and Grant T. Chartrand



- From Measuring Achievement to Capturing Learning:
  - Capturing richer evidence of learning contexts.
  - Capturing broader evidence of individual learning.
  - Capturing evidence of social learning.
  - Capturing evidence from learning pathways.
- From Credentialing Graduates to Recognizing Learning.
- From Accrediting Schools to Endorsing Learning.

mozilla OpenBadges

2017

1EDTECH

Credly

2022

Credly by Pearson

badgr

2022

CANVAS Credentials

CONCENTRIC SKY

INSTRUCTURE

Major **Recent Developments** from Current Badge Community Leaders

- *Digital Credentials Consortium* (DCC):
  - Creating new open-source tools.
- Cross-compliant metadata standards:
  - *Open Badges Infrastructure* (OBI) 3.0.
  - WC3's *Verifiable Credentials.*
  - 1EdTech's *Comprehensive Learner Record* (CLR).
  - Credentials are now cryptographically signed.
- Learning and employment records (LER):
  - *LER Ecosystem Map.*
  - *Learn & Work Ecosystem Library.*

Kerrie Lemoie
Director of Digital Credentials Consortium

Nate Otto
Consultant, Badgr Creator

Noah Geisel
UC Boulder
Manager of Micro-Credentials Program

Major **Recent Trends** from Current Badge Community Leaders

- Well over 100M open badges issued:
  - New badge on LinkedIn every 60 seconds.
- Skills-Based Hiring.
  - SkillsFWD Grants.
- “Alignment” means more interoperability and transfer of competencies.
- “Evidence” adds trust by demonstrating how criteria were met.
- New crop of vendors and open source software

Kerrie Lemoie
Director of Digital Credentials Consortium

Nate Otto
Consultant, Badgr Creator

Noah Geisel
UC Boulder
Manager of Micro-Credentials Program


PURDUE
GLOBAL
Cybersecurity
Fundamentals


MINNESOTA STATE
IT Center of Excellence
INTRODUCTION
TO CYBERSECURITY
PROFICIENT


KELLEY SCHOOL OF BUSINESS
SPACE CYBERSECURITY


Microsoft
CERTIFIED
CYBERSECURITY
ARCHITECT
EXPERT

MENU

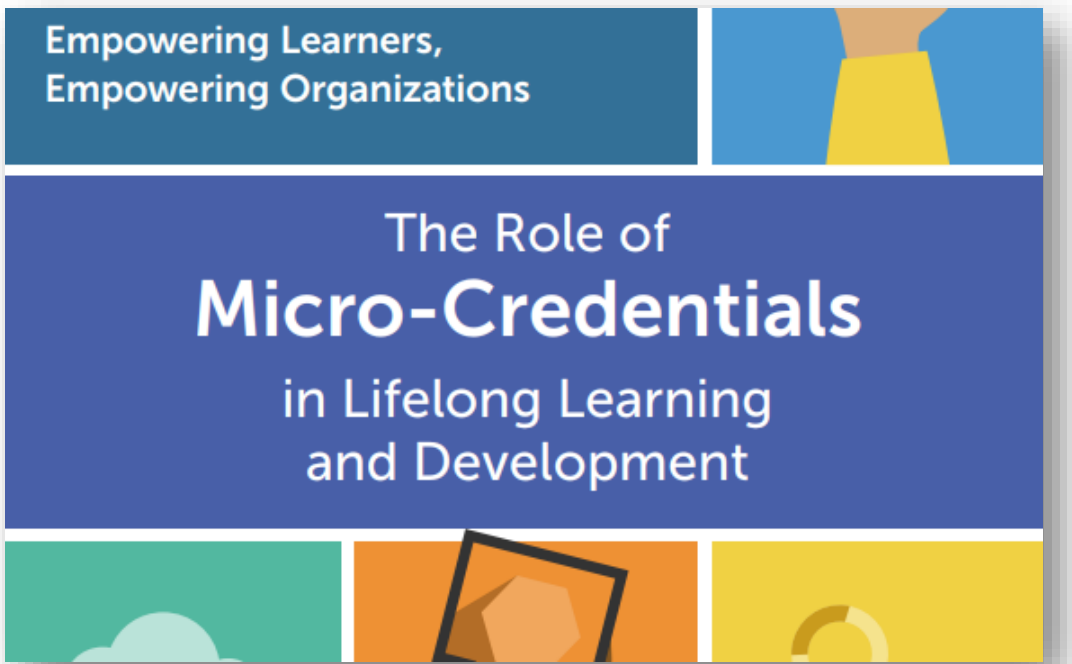
Florida Gulf Coast University > FGCU Digital Badges >
Digital Badge Summit

Learn and Network at the Digital Badge Summit at FGCU

Florida Gulf Coast University welcomes you to join a two-day Badging Summit on-site at our beautiful campus in Fort Myers, FL. This summit will bring peer institutions together to network, learn, and share about badging programs of all sizes.

Digital Promise®

Accelerating Innovation in Education



The Promise of Micro-credentials and Learning and Employment Record Technologies for Youth and K-12 Schools

Contributing Authors: Zohal Shah, Marilys Galindo, Chioma Aso-Hernandez, Christina Luke Luna, Keun-woo Lee, Josh Weisgrau, Teresa Solorzano, Britney Jacobs

August 2024

Open Badges and Cybersecurity Research

- Pike, R. E., Brown, B., West, T., & Zentner, A. (2020). Digital Badges and E-Portfolios in Cybersecurity Education. *Information Systems Education Journal*, *18*(5), 16-24.
- Brown, E., & Hubbard, Z. (2023, June). *Developing Micro-credentials to Infuse Cybersecurity into Technician Education*. American Society for Engineering Education annual conference.
- Chakravorty, D. K., Lawrence, R., He, Z., Brashear, W., Liu, H., Palughi, A. J., ... & Palsole, S. V. (2023). Access to Computing Education Using Micro-Credentials for Cyberinfrastructure. *Journal of Computational Science*, *14*(2).

New Cybersecurity Learning Transfer Research

- Hickey, D. T., and Kantor, R. (2023). Contrasting **cognitive theories** of learning transfer to advance cybersecurity instruction, assessment, and testing. *The Journal of Cybersecurity Education Research and Practice.*
- Hickey, D. T., & Kantor, R. J (in revision). Transforming cybersecurity and computing education with **personal authenticity and situative** transfer.
- Hickey, D. T., & Kantor, R. J (in revision). Evolving and emerging theories of transfer and **culturally sustaining** cybersecurity education and training.

Thank You Very Much!!!

- https://bit.ly/RMAbadges
- dthickey@iu.edu

Q&A

Are There Any Questions?

Making Sense of Cyber Risk Metrics – Communicating to the Board and Committees

Carol Sterino

Director, Technology Risk Management
Depository Trust & Clearing Corporation (DTCC)

Making Sense of Cyber Risk Metrics, Communicating to the Board and Committees

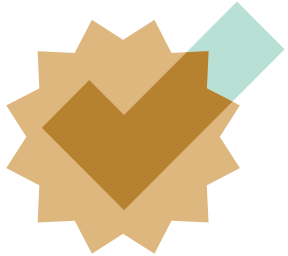
NIST - FISSEA FALL FORUM

PRESENTER: Carol Sterino
DATE: September 17, 2024
DEPARTMENT: Cyber Security & Technology Risk Management

Agenda

I. Tips for Communicating
II. Comprehensive Risk Analysis Summarized
III. Steps to Summarization

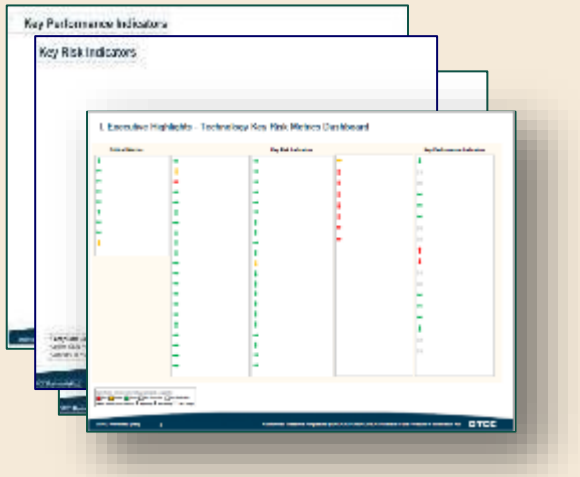
I. Tips for Communicating



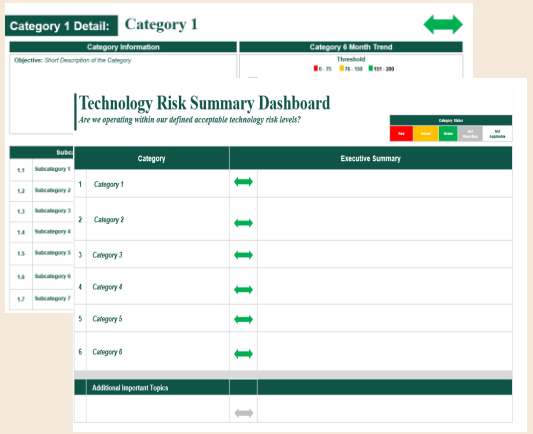
- Keep It Simple
- Consolidate Information
- Highlight Key Topics
- Be Prepared to Speak to the Details
- One Size Does Not Fit All

II. Comprehensive Risk Analysis Summarized

- Programs maturity led to exponential growth in data and metrics
- Required an approach to summarize large amounts of information
  - Leveraged a framework *(ie NIST CSF!)*
- Enhanced reporting quality while reducing the complexity and volume of data



Largest Report Supported Monthly
100+ metrics; 120+ report pages



Committee(s) Report(s) Supported Monthly
6-7 Categories; 2-8 report pages

*Disclaimer – sample data; for presentation purposes only, not for re-use or republication of any kind

III. Steps to Summarization

1. Data Identification and Mapping

2. Data Normalization

3. Scoring Process

4. Threshold Determination

5. Risk Evaluation

1. Data Identification and Mapping

1. Metric analysis performed & aligned with (NIST) Framework

2. Mapped metrics to internal metric reporting hierarchy

3. Socialized list with key stakeholders

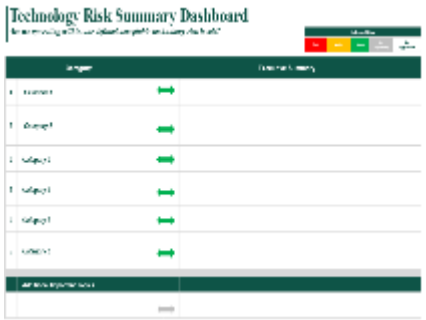
4. Obtained buy in

5. Final hierarchical reporting list published

Metrics
≥ 1 Mapped to a Subcategory

Subcategories
≥ 1 Mapped to a Category

Categories
Top level



*Disclaimer – sample data; for presentation purposes only, not for re-use or republication of any kind

2. Data Normalization

Data Normalization is used to compare and consolidate unlike metrics

1. Only the common output status of Red, Amber and Green is retained from detailed metric reporting
2. RAG statuses are assigned a Normalized Data Value, in this case: 0, 100 and 200
3. After Data Normalization, **Metric 1** has a Normalized Data value of 200 as its RAG status is Green

Normalized Data Value = *(Metric's RAG Status + RAG Normalization Value)*

BEFORE **NORMALIZATION**

Metric	Metric Thresholds	Metric Data & RAG Status
Metric 1	**Green: ≥90% to ≤100%** Amber: ≥80% to <90% Red: <80%	95%
Metric 2	Green: ≥0 to <10 Amber: ≥10 to <15 Red: ≥15	13
Metric 3	Green: ≥0 to <5 Amber: ≥5 to <10 **Red: ≥10**	11
Metric 4	Green: ≥90% to ≤100% Amber: ≥80% to <90% **Red: <80%**	75%

1

2

RAG Status / Normalized Data Value	
Red	0
Amber	100
Green	200

AFTER **NORMALIZATION**

Metric	Metric RAG Status	Normalized Data Value only
Metric 1		**200**
Metric 2		**100**
Metric 3		**0**
Metric 4		**0**

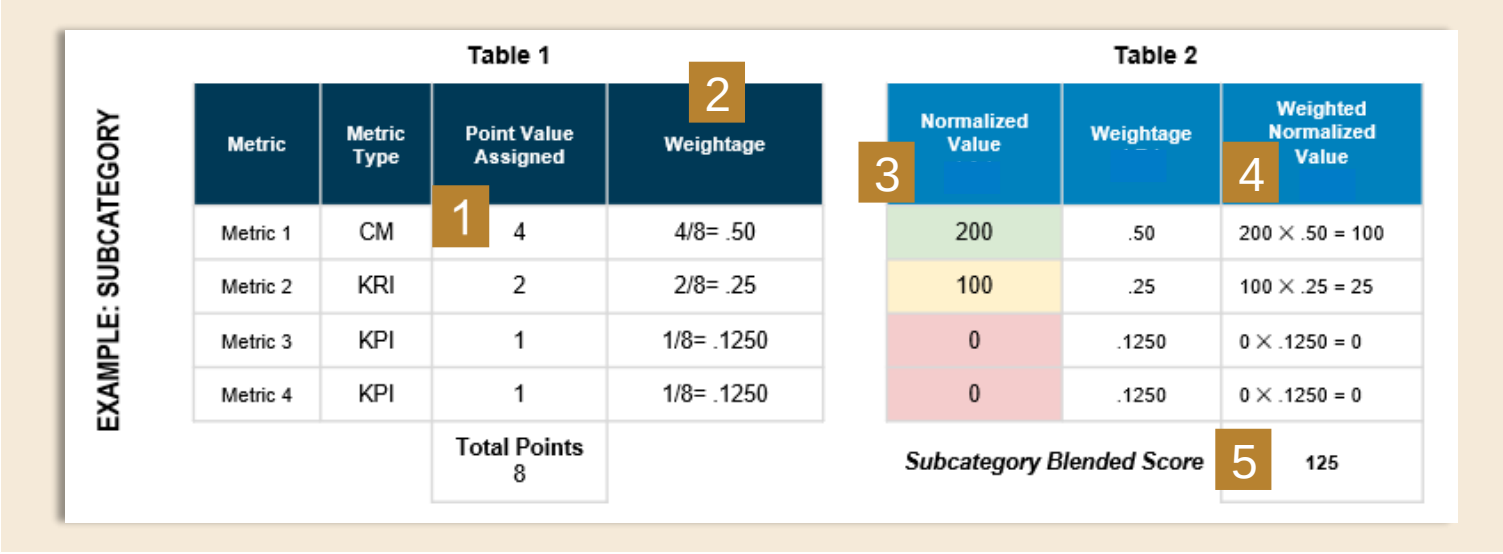
3

3. Scoring Process

Blended Score is calculated for each Subcategory and Category

1. Metric Point Value = in this case, based on metric type
2. Metric Weightage = *(Metric Point Value / Total Metric Value Points)*
3. Metric Normalized Value = RAG status' Normalized Data Value
4. Metric Weighted Normalized Value = *(Metric Normalized Value * Metric Weighted Value)*
5. Subcategory Blended Score = *(Sum all Metrics Weighted Normalized Value)*

   Category Blended Score - based on the number of Subcategories included and the weight of each Subcategory which is determined by the highest metric point value within the Subcategory.



4. Threshold Determination

One standardized threshold established for all Categories and Subcategories

- Evaluated use customized thresholds
- Analyzed average, median and mode
- Analyzed historical metric data

Single Threshold for all Categories and Subcategories		
Red **0 – 75**	**Amber** **75 – 150**	**Green** **151 – 200**

5. Risk Evaluation

1., 2. RAG status is determined by applying the Blended Score to the threshold range.

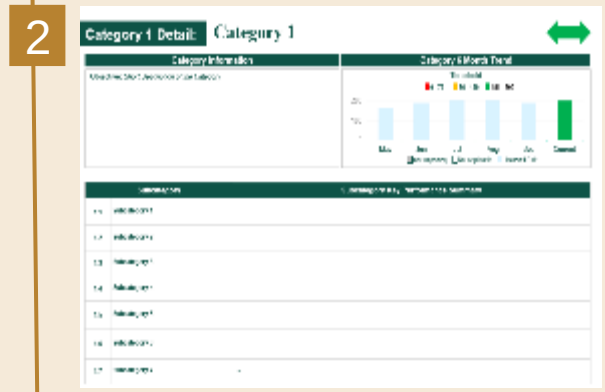
3. The RAG trend is based on the prior month's RAG status.

- Methodology is not 100% quantitative; qualitative SME evaluation and adjustment as required

EXAMPLE: CATEGORY

Threshold		
Red 0 – 75	**Amber** 75 – 150	**Green** 151 – 200

Subcategory	Metric Type	Normalized Values	Weightage	Weighted Normalized Value
Sub 1	CM	200	.50	200 × .50 = 100
Sub 2	KRI	100	.25	100 × .25 = 25
Sub 3	KPI	200	.1250	200 × .1250 = 25
Sub 4	KPI	200	.1250	200 × .1250 = 25
		Category Blended Score		**175**
Apply Category Blended Score to Category Threshold for RAG Status to plot on Category Detail Page				**175**



1

2

3

Thank You

Q&A

Are There Any Questions?

CMMI: A Practical End User Implementation of Process Improvement in Security Awareness Training

Dr. Natalie Foster Johnson
Founder and Researcher
CyberMINDS Research Institute

Dr. Alexis Perdereaux-Weekes
Co-Founder and Sr. Managing Partner
CyberMINDS Research Institute

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

CYBERMinds

Leveraging CMMI for Enhanced Security Awareness Training: A Practical Approach to Process Improvement

Enhancing Cybersecurity Resilience through Structured Training Programs

Dr. Natalie Foster Johnson and Dr. Alexis Perdereaux-Weekes

September 17, 2024

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Dr. Natalie Foster Johnson

Dr. Alexis Perdereaux- Weekes

CYBERMinds

CyberMINDS Research Institute

The thought leaders in information security, cyber, and privacy protection.

www.cybermindsinstitute.org

Introduction

Overview of CMMI:

- What is CMMI? (***Capability Maturity Model Integration CMMI)***
- Importance in process improvement

CMMI in Cybersecurity

- Structured approach is particularly valuable in standardizing security practices, including security awareness training.

Relevance to Security Awareness Training:

- Helps organization transition from an ad-hoc, reactive methods to standardized, measurable and proactive processes.

Capability Maturity Model Integration (CMMI):

https://insights.sei.cmu.edu/library/cmmi-for-development-version-13/

CMMI Framework for Security Training

Standardized Approach:

- Background and evolution of the Framework
- Adoption and effective approaches to implementation
- Integration with Organizational Processes
- CMMI brings consistency to security awareness training

CMMI's Role in Cybersecurity:

- Structured Process Improvement
- Risk Management Integration
- Organizational Prioritization of Security Responsibilities
- Measurement and Metrics Standardization
- Tracking and enhancing training effectiveness

Making the case for Process Improvement in Security Awareness Training

Why Security Awareness Training Matters?

- Cultivates a Security-Conscious Culture
- Enhances Process Maturity
- Alignment with Risk Management Outcomes
- Promotes Compliance and Best Practices Adoption at all levels of the organization

Challenges with Traditional Training:

- Ad-hoc and reactive approaches
- One-Size Fits approach over utilized.
- Lack of standardization
- Inability to measure outcomes in an evolving threat landscape

Leveraging CMMI Processes for Security Training

Standardized Framework:

- CMMI provides consistency in training

Process Implementation:

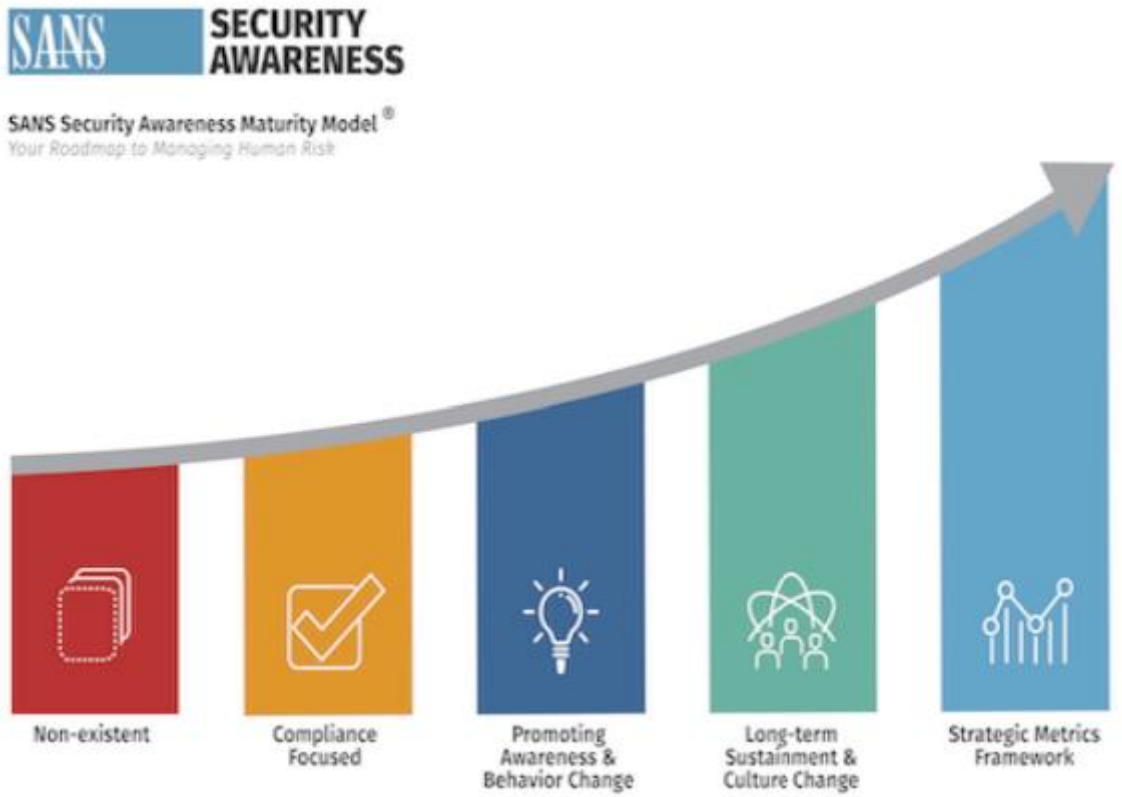
- Establishing a systematic approach to security awareness

Transformation of Training Programs:

- From reactive to proactive and standardized methods

Real-World Example 1

Case Study 1: SANS Security Awareness



https://www.sans.org/security-awareness-training/resources/maturity-model/

Real-World Example 2

FEDERAL INFORMATION SECURITY EDUCATORS
FISSEA

CYBERMinds

Case Study 2: Cyber-Competency Health and Maturity Progression Framework (CHAMP):

https://factsheets.inl.gov/FactSheets/Cyber-CHAMP.pdf

Awareness	**Awareness** – Represents individual that only need to have a level of cybersecurity concepts and understanding that are cognizance in nature. Contain simple knowledge or perceptions of security concepts.
Support	**Support** – A knowledge of foundational security concepts and entry-level technical skill sets. An individual at this level may also have some tactical break and fix responsibilities.
Maintain	**Maintain** – Competency is founded in functional security concepts. An individual can address tactical break and fix situations as well as take a proactive, supportive role in identifying department technical needs.
Implement	**Implement** – Employees often considered by peers and leadership as an SME in their field. They express complex technical concepts effectively and are responsible for identifying technical needs across the organization.
Design	**Design** - Individuals that understand the big picture and how actions affect system interoperability. Demonstrate strong presentation skills, possess strategic-planning skills, and manage large projects.

Benefits of CMMI in Security Awareness Training

Value Additions:

- **Consistency & Standardization**: Ensuring uniform understanding of security protocols.
- **Long-term Impact**: Building a resilient organization with continuous training improvements.
- **Measurable Success**:
  - Demonstrating the impact of CMMI on incident response times and employee readiness.
  - Moving from reactive to proactive training
  - Enhanced Process Consistency

Strategic Rationale for CMMI Implementation

Supporting Organizational Goals:

- Aligning security awareness with business objectives
- Enable the organization to measure readiness to address threats

Enhancing Maturity of Training Programs:

- Steps toward a mature and resilient training environment
- Expansion of risk mitigation capability across the organization
- Individualize responsibilities to address threats beyond the IT function

Conclusion

Summary of Key Points:

- Recap of CMMI integration into security awareness training
- Importance of maturity in training programs
- The strategic impact of CMMI on long-term cybersecurity resilience

Call to Action:

- Encouraging organizations to adopt CMMI principles and strategies for better outcomes
- Establishing measurements of program effectiveness, understanding what “Works” and “Where Improvements are Needed”

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

CYBERMinds

Questions & Answers

THANK YOU!

Contact US: Inquiry@cybermindsinstitute.org

Federal Information Security Educators (FISSEA) Fall Forum

BREAK

The Forum will resume at 3:05pm ET

#FISSEA | nist.gov/fissea

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Welcome Back!

Brooke Crisp
FISSEA Co-Chair

Cybersecurity - Metrics Measuring Beyond Compliance Requirements

Tayo O. Olagunju
Federal Aviation Administration
Air Traffic Organization Cybersecurity Group

FAA - Air Traffic Organization Cybersecurity Group (ACG Cyber Test Team, AJW-B44)

Cybersecurity - Metrics Measuring Beyond Compliance Requirements

Presented to: National Institute of Standards and Technology (NIST)

By: Mr. Tayo Olagunju, FAA ACG Cyber Test Team Manager

Date: 17 September 2024

Federal Aviation Administration

Agenda

- Introduction and Overview
- Employee Awareness and Engagement
- Incident Response and Management
- Behavioral Metrics
- Threat and Vulnerability Management
- Policy and Governance
- Cultural Indicators
- Performance Metrics
- Innovation and Improvement
- Other Considerations: Implementing a Holistic Measurement Approach

Introduction and Overview

Measuring the effectiveness of a cybersecurity culture goes beyond mere compliance with regulations and standards. To truly refine and strengthen cybersecurity culture, organizations need to track specific metrics that provide deeper insights into the behaviors, attitudes, and effectiveness of security measures within the organization. Here are some key metrics to consider:

Employee Awareness and Engagement

- **Phishing Simulation Results:** Measure the success rate of phishing simulations to determine how well employees can recognize and avoid phishing attacks.
  - Source: Phishing awareness training responses and Cyber Training quiz responses
- **Training Completion Rates:** Track the percentage of employees who complete cybersecurity training programs and how often they participate in refresher courses.
  - Source: Periodic Cyber Training compliance statistics
- **Knowledge Assessments:** Evaluate employee understanding of cybersecurity principles through regular quizzes and assessments.
  - Source: Cyber Training quiz responses

Incident Response and Management

- **Incident Detection Time:** Measure the average time taken to detect a cybersecurity incident from the moment it occurs.
  - Source: SOC or CIRT incident detection stats
- **Incident Response Time:** Track the time it takes for the incident response team to respond to and mitigate security incidents.
  - Source: SOC or CIRT incident response stats
- **Post-Incident Analysis:** Evaluate the thoroughness and effectiveness of post-incident analysis and reporting, including lessons learned and applied improvements.
  - Source: SOC or CIRT incident response stats
  - Cyber exercise and training AAR stats

Behavioral Metrics

- **Multi-Factor Authentication (MFA):** Increases the complexity of identity management security
  - Source: Compliance with EO 14058 stats
- **Password Hygiene:** Monitor the use of strong, unique passwords and the frequency of password changes among employees.
  - Source: Policy compliance and audit stats
- **Access Control Violations:** Track unauthorized access attempts and instances of privilege misuse or escalation, including implementation of Zero Trust strategy
  - Source: Privilege violations, audit, and invalid logon attempts
- **Device Security Compliance:** Measure adherence to security policies regarding device use, such as encryption and secure configurations.
  - Source: Audit and policy compliance records

Failures to tightly enforce established security policy requirements were contributing factors in all major U.S. cyber incidents including last year’s MGM Resort disruption and the Caesars data exfiltration

Threat and Vulnerability Management

- **Vulnerability Remediation Time:** Measure the time it takes to remediate identified vulnerabilities after they are discovered. (SLA/patch severity, LOE)
  - Source: Include patch compliance duration to periodic patch management reporting
- **Patch Management Efficiency:** Track the speed and effectiveness of deploying patches and updates across systems and applications.
  - Source: Include patch deployment failure (especially SU server, suss.exe)
- **Threat Intelligence Utilization:** Evaluate how effectively threat intelligence is integrated into security strategies and decision-making processes.
  - Source: Establish and codify all commercial (McAfee, Mandiant, etc.) and US Gov (DoD, IC, DHS, etc.)
  - Source: Tie reported threats to deployed mitigation measures and incidents

Policy and Governance

- **Policy Compliance Rates:** Monitor adherence to cybersecurity policies and procedures across the organization.
  - This is especially important for cloud or other hosting environments and it should be recognized that hosted systems inherit those risks. This also applies to vendor provided systems and applications. Compliance issues would be codified in contracts or Service Level Agreements. This often leads to complex negotiations and enforcement clauses involving contracting specialists who are not cyber savvy.
- **Audit Findings:** Analyze the number and severity of findings from internal and external audits, and track improvements over time.
  - Valid and available audit data supports multiple cyber monitoring, alerting, and analytical functions
- **Third-Party Risk Management:** Evaluate the effectiveness of managing risks associated with third-party vendors and partners.
  - Risk posed by sub-contractors or third-party suppliers must also be codified in contractual agreements establishing responsibility and accountability. Especially important given the implications of the Rev5 Supply Chain Controls.

Cultural Indicators

- **Security-Related Feedback:** Collect and analyze feedback from employees on cybersecurity policies, practices, and the overall security culture.
  - Sources: Employee questionnaires, exercise AARs, compliance assessment interviews, incident reports
- **Cross-Department Collaboration:** Measure the level of collaboration between IT, security, and other departments in implementing security initiatives.
  - Are relationships adversarial or supportive? Is communication frequent or only as required?
- **Leadership Involvement:** Evaluate the extent of leadership involvement in promoting and supporting cybersecurity initiatives and culture.
  - Are Executive Leaders and supporting managers advocates for cyber mission, policy, and funding
  - Do strategic organizational decisions balance cybersecurity concerns and risks?

Performance Metrics

- **Security Incident Frequency:** Track the number of security incidents over time to assess trends and patterns.
  - Source: SOC or CIRT incident stats
- **False Positives and Negatives:** Measure the accuracy of security tools in identifying real threats versus false positives or negatives.
  - Source: External facing Firewall/IPS logs
- **Cost of Security Incidents:** Calculate the financial impact of security incidents, including remediation costs, downtime, and potential reputational damage.
  - Holistic costs not limited to IT, also include operational (outage, loss of services), training, and insurance

Innovation and Improvement

- **Adoption of New Technologies:** Track the implementation and impact of new cybersecurity technologies and tools within the organization.
  - Engrain cybersecurity in IT acquisition processes to ensure new tech (e.g. cloud and AI) are sound investments and include cyber capabilities that are expandable throughout the system's lifecycle
- **Continuous Improvement Initiatives:** Measure the effectiveness of continuous improvement programs in enhancing cybersecurity practices and culture.
  - Include personnel management and training for current employees and recruiting efforts
- **Innovation in Security Practices:** Evaluate the organization's ability to innovate and adapt security practices to emerging threats and challenges.
  - Top to bottom holistic, and objective, assessments based on sound metrics

Other Considerations: Implementing a Holistic Measurement Approach

1. **Develop a Comprehensive Framework**
    - **Balanced Scorecard:** Use a balanced scorecard approach to track and analyze a range of metrics that align with organizational goals and objectives.
    - **KPIs and Benchmarks:** Establish key performance indicators (KPIs) and benchmarks to measure progress and performance over time.
2. **Utilize Advanced Analytics**
    - **Data Analysis Tools:** Leverage data analytics tools to gather insights from security data and identify trends, patterns, and areas for improvement. (cloud analytics)
    - **Dashboard Reporting:** Implement dashboard reporting to provide real-time visibility into cybersecurity performance and metrics. (what matters? Enable awareness/decision making)

Other Considerations (Continued)

1. **Foster a Culture of Continuous Improvement**
   - **Feedback Mechanisms:** Implement feedback mechanisms to gather input from employees and stakeholders on cybersecurity initiatives and culture.
   - **Iterative Learning:** Encourage iterative learning and adaptation by regularly updating training programs and security practices based on feedback and metrics.
2. **Engage Leadership and Stakeholders**
   - **Leadership Commitment:** Ensure leadership commitment to cybersecurity initiatives by involving them in setting goals, reviewing metrics, and driving cultural change.
   - **Stakeholder Involvement:** Engage stakeholders across the organization to support and contribute to cybersecurity efforts and cultural refinement.
3. **Conduct Regular Reviews and Assessments**
   - **Quarterly Reviews:** Conduct regular reviews and assessments of cybersecurity metrics to evaluate progress and identify areas for improvement.
   - **External Audits:** Consider external audits to provide an objective evaluation of cybersecurity practices and culture.

Questions and Discussion

Demo of Cybersecurity and Infrastructure Security Agency (CISA) Videos

Anastacia “Staci” Webster

Academic Programs Lead
Cybersecurity and Infrastructure
Security Agency (CISA)

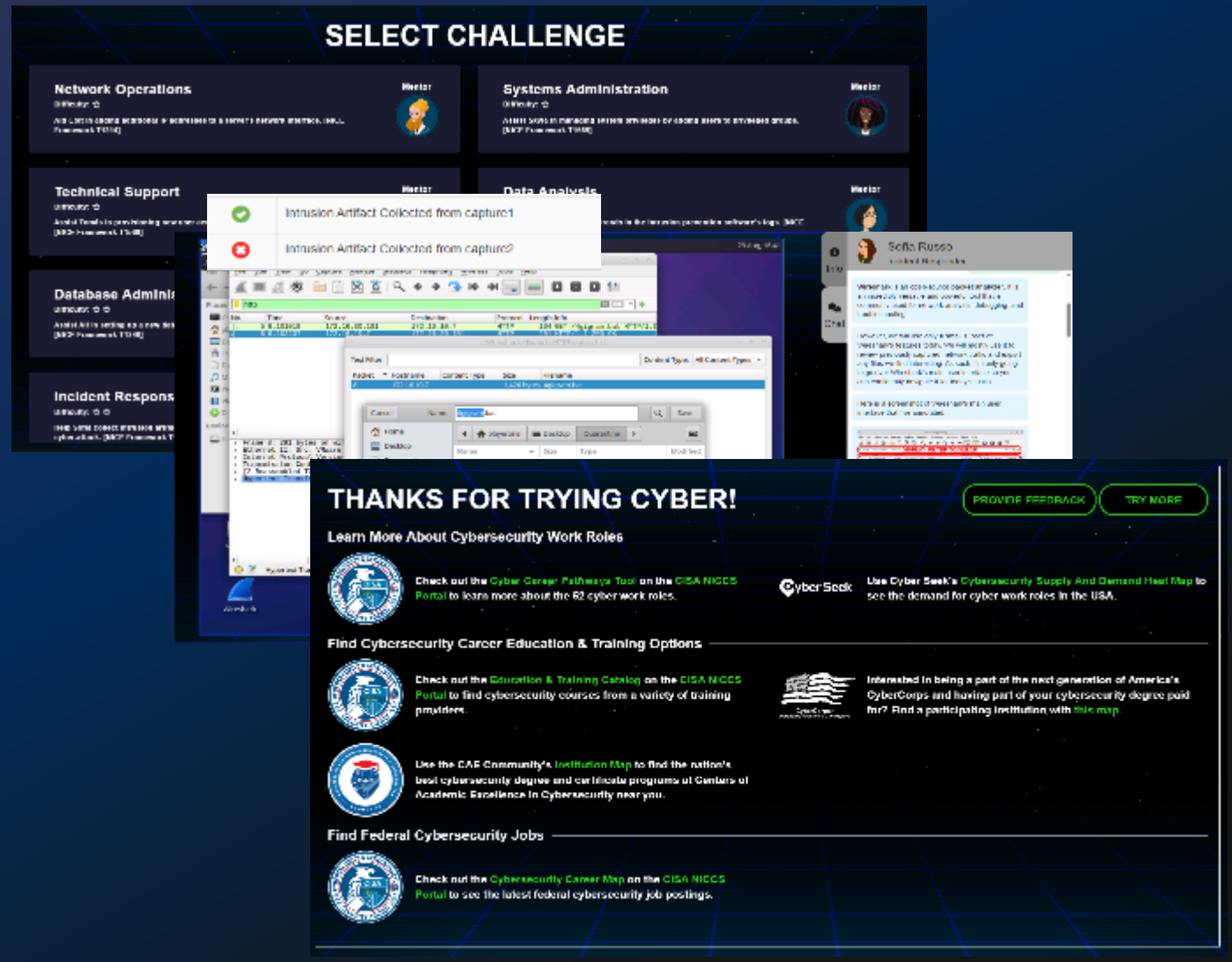

TRY
CYBER

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Try Cyber

14 Micro-Challenges, 10 Workforce Roles

Developed as resources for cybersecurity awareness and career exploration supporting the Cyber Careers Pathway Tool on the National Initiative for Cybersecurity Careers and Studies (NICCS®) website. The micro-challenges are quick, 15-minute, hands-on experiences that put users into cybersecurity workforce. **26,000+ user attempts since launch!**



15 Micro-Challenges (planned development)

Development will begin in 2025 to include both technical and non-technical cyber workforce roles.

TRY CYBER

https://trycyber.us/

Contact us: Education@cisa.dhs.gov

Q&A

Are There Any Questions?

Fireside Chat and Cybersecurity Awareness Month Preparation

Laura Edwards
Awareness and Outreach Section Chief
Cybersecurity and Infrastructure Security Agency (CISA)

Jennifer Cook
Senior Director of Marketing
National Cybersecurity Alliance

Closing Remarks

Marian Merritt
Deputy Director NICE
National Institute of Standards and Technology

Frauke Steinmeier
FISSEA Co-Chair

Get Involved

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

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

SAVE THE DATE

Federal Information Security Educators (FISSEA) Conference

May 13-14, 2025

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

THANK YOU

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

https://www.surveymonkey.com/r/fisseafallforum2024

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA