fissea

FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

LOOKING FORWARD | CYBERSECURITY TRAINING TO MEET THE NEW CHALLENGES

FEDERAL INFORMATION SECURITY EDUCATORS

SPRING FORUM

MAY 17, 2022
1:00PM - 4:00PM ET

#FISSEA2022 | NIST.GOV/FISSEA

WELCOME AND OPENING REMARKS

Susan Hansche

FISSEA Co-Chair

Cybersecurity & Infrastructure Security Agency

Department of Homeland Security

FISSEA SPRING FORUM

LOOKING FORWARD | Cybersecurity Training to Meet the New Challenges

GET INVOLVED

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

Volunteer for the Planning Committee
Email FISSEA@nist.gov

Serve on the Contest or Award Committees for 2022

FISSEA FALL FORUM THEME: ROLE BASED TRAINING

Submit your proposals now for the Ignite Presentations

(7–8minute lightning rounds)

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

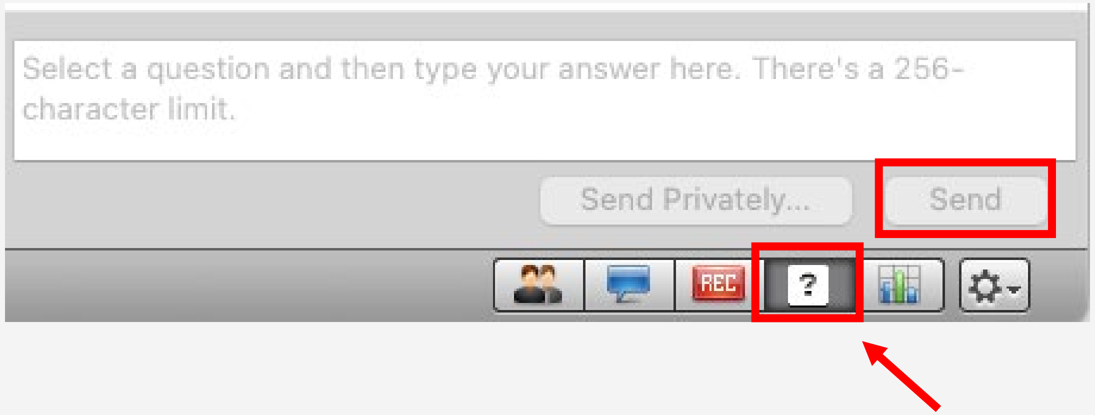
Priority Consideration: September 1, 2022, 11:59 PM ET

Do you manage a Role Based Training Program?

The NIST SP 800-50 Co-Author team would like to interview you.
Please email Marian.Merritt@nist.gov to learn more.

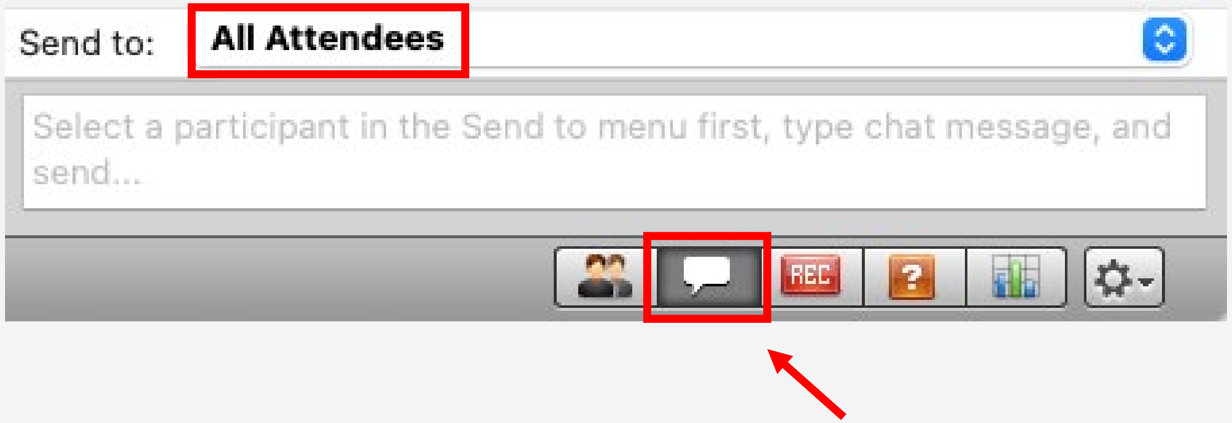
ENGAGE DURING THE EVENT

- **Please use the Q&A to send questions for the speakers**. Be sure to click the “send” button after typing your question. We will do our best to answer all questions.



Select a question and then type your answer here. There's a 256-character limit.

- **Please use the CHAT to make comments and share information** with other attendees. Please remember to not use the chat space for promoting any commercial products or services.



Send to: All Attendees

Select a participant in the Send to menu first, type chat message, and send...

KEYNOTE: *A Whole Lotta BS (Behavioral Science) About Cybersecurity*

○○○○

Lisa Plaggemier

Executive Director

National Cyber Security Alliance

○○○○

NATIONAL
CYBERSECURITY
ALLIANCE

Reach

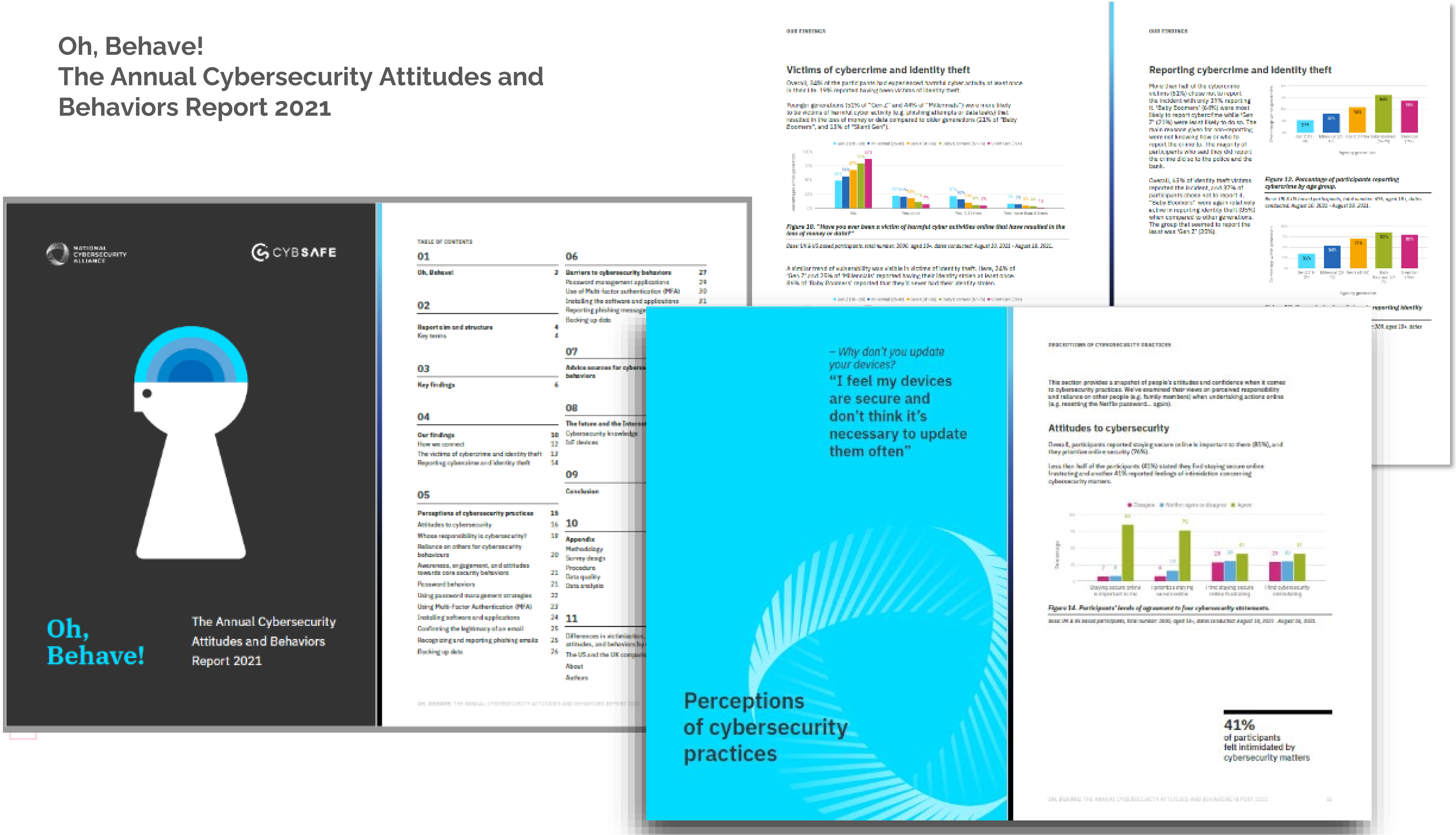
Millions of people turn to the National Cybersecurity Alliance for information

- 2+ million pageviews StaySafeOnline.org
- 370,000+ social media followers
- 150+ free resources
- Thousands of webinar attendees

NATIONAL
CYBERSECURITY
ALLIANCE

84 MILLION

Oh, Behave!
The Annual Cybersecurity Attitudes and Behaviors Report 2021



NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE

Oh, Behave!

The Annual Cybersecurity Attitudes and Behaviors Report 2021

TABLE OF CONTENTS

OH, BEHAVE! THE ANNUAL CYBERSECURITY ATTITUDES AND BEHAVIORS REPORT 2021

OUR FINDINGS

Victims of cybercrime and identity theft

Overall, 34% of the participants had experienced harmful cyber activity at least once in their life. 19% reported having been victims of identity theft.

Younger generations (51% of "Gen Z" and 44% of "Millennials") were more likely to be victims of harmful cyber activity (e.g. phishing attempts or data leaks) that resulted in the loss of money or data compared to older generations (21% of "Baby Boomers", and 13% of "Silent Gen").

Figure 10. "Have you ever been a victim of harmful cyber activities online that have resulted in the loss of money or data?"

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

A similar trend of vulnerability was visible in victims of identity theft. Here, 24% of 'Gen Z' and 25% of 'Millennials' reported having their identity stolen at least once. 86% of 'Baby Boomers' reported that they'd never had their identity stolen.

OUR FINDINGS

Reporting cybercrime and identity theft

More than half of the cybercrime victims (62%) chose not to report the incident with only 37% reporting it. 'Baby Boomers' (64%) were most likely to report cybercrime while 'Gen Z' (21%) were least likely to do so. The main reasons given for non-reporting were not knowing how or who to report the crime to. The majority of participants who said they did report the crime did so to the police and the bank.

Overall, 63% of identity theft victims reported the incident, and 37% of participants chose not to report it. "Baby Boomers" were again relatively active in reporting identity theft (85%) when compared to other generations. The group that seemed to report the least was 'Gen Z' (35%).

Figure 12. Percentage of participants reporting cybercrime by age group.

Base: UK & US based participants, total number: 691, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

reporting identity

308, aged 18+, dates

– Why don't you update your devices?

"I feel my devices are secure and don't think it's necessary to update them often"

Perceptions of cybersecurity practices

PERCEPTIONS OF CYBERSECURITY PRACTICES

This section provides a snapshot of people's attitudes and confidence when it comes to cybersecurity practices. We've examined their views on perceived responsibility and reliance on other people (e.g. family members) when undertaking actions online (e.g. resetting the Netflix password... again).

Attitudes to cybersecurity

Overall, participants reported staying secure online is important to them (85%), and they prioritize online security (76%).

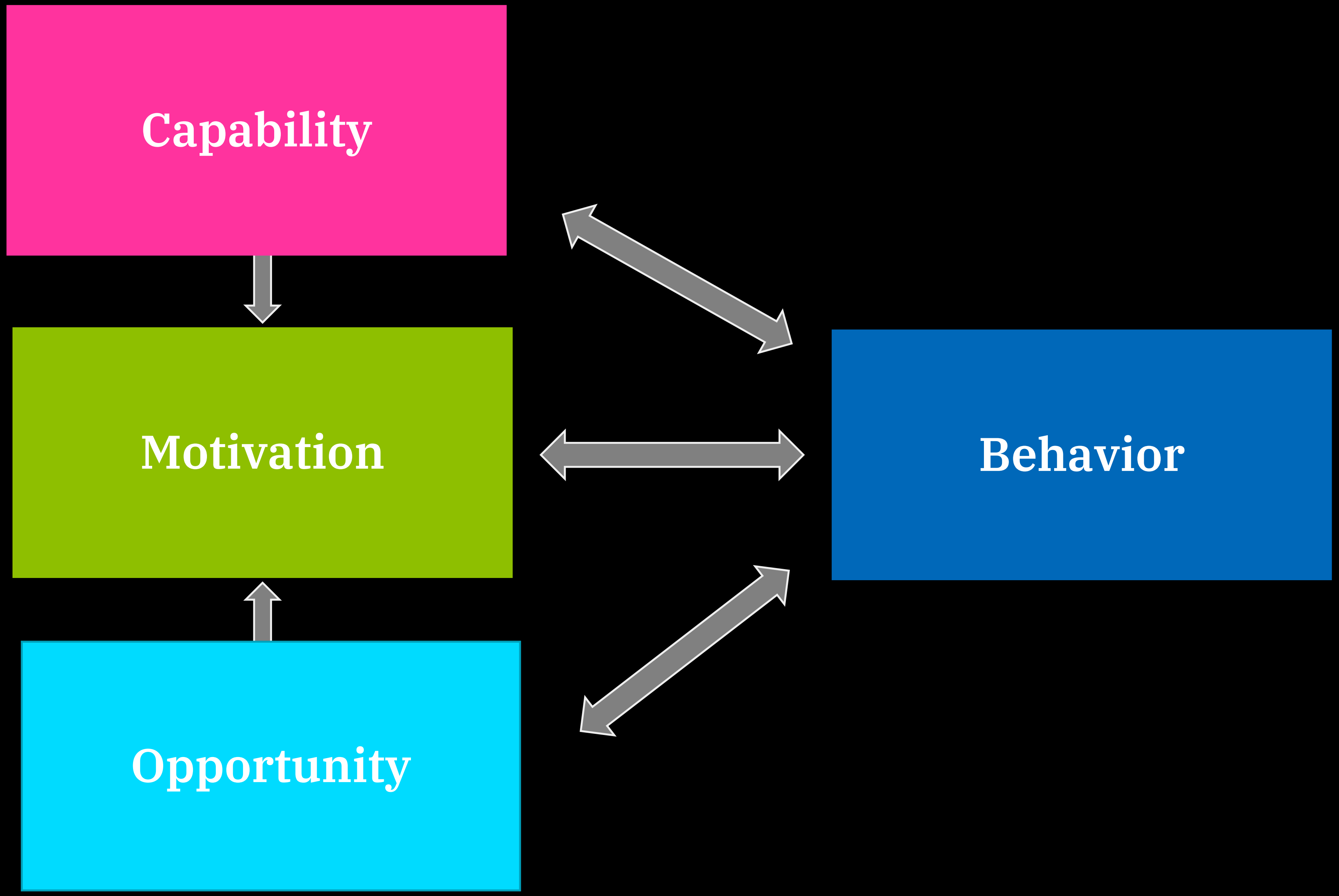
Less than half of the participants (41%) stated they find staying secure online frustrating and another 41% reported feelings of intimidation concerning cybersecurity matters.

Figure 14. Participants' levels of agreement to four cybersecurity statements.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

41%
of participants
felt intimidated by
cybersecurity matters

■ Gen Z (18 - 24) ■ Millennial (25-40) ■ Gen X (41-56) ■ Baby Boomers (57-75) ■ Silent Gen (76+)
100%
75%
50%
25%
0%
40%
50%
67%
72%
80%
No
Yes, once
Yes, 2-3 times
Yes, more than 4 times
21%
32%
42%
64%
55%
Age by generation
35%
54%
71%
85%
80%
■ Disagree ■ Neither agree or disagree ■ Agree
Percentage
7
8
85
8
16
76
29
30
41
29
30
41
Staying secure online is important to me
I prioritize staying secure online
I find staying secure online frustrating
I find cybersecurity intimidating



Capability

Motivation

Opportunity

Behavior

Security Behaviors

i) creating and managing passwords;

ii) applying Multi-Factor Authentication (MFA);

iii) installing the latest updates;

iv) checking message legitimacy (phishing);

v) recognizing and reporting phishing, and

vi) backing up data.

> “People are irrational and they usually make decisions that have nothing to do with facts. And yet we spend most of our time improving our facts and very little concerned with the rest.”

Seth Godin

Feelings

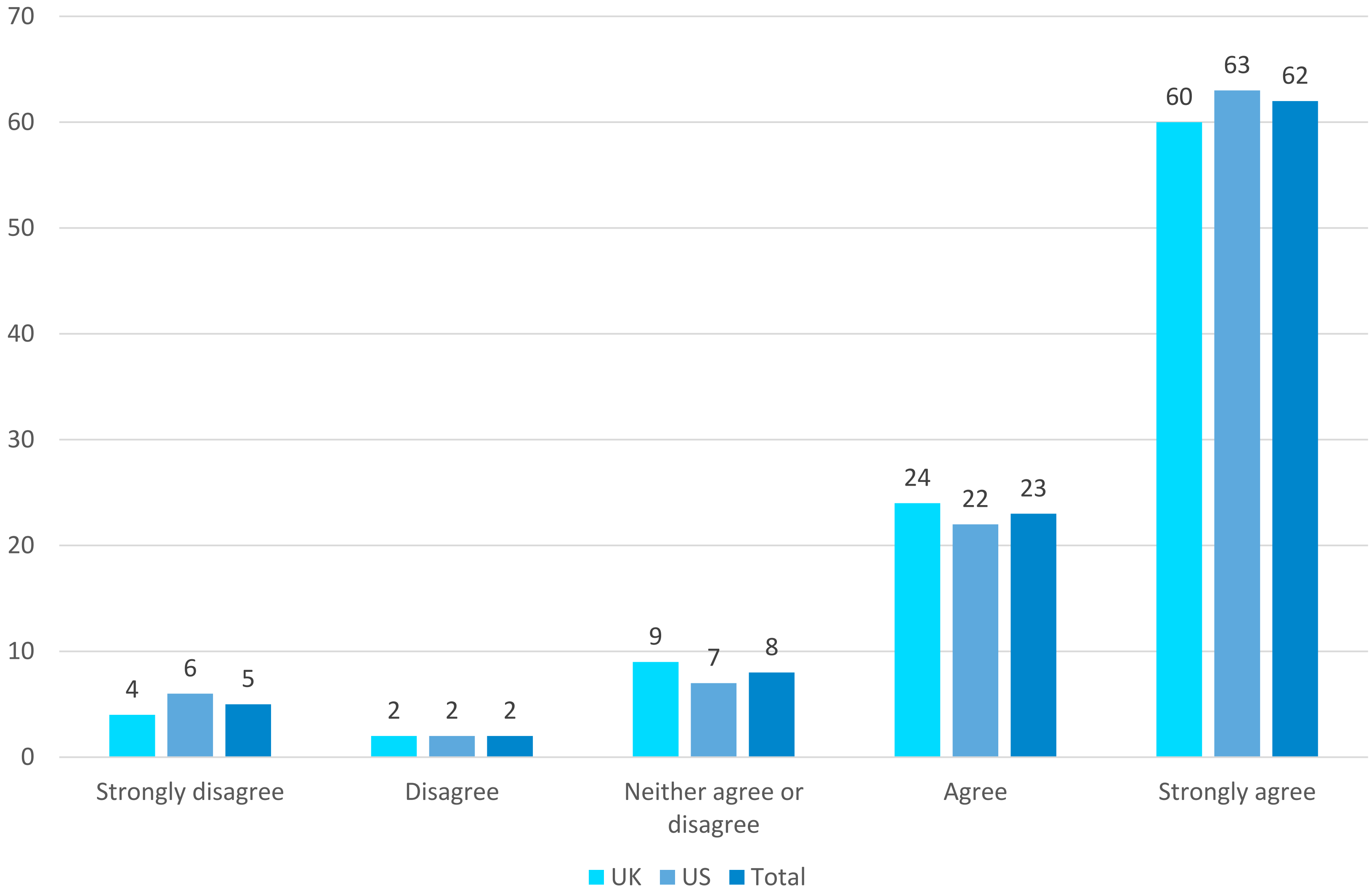
Importance of staying secure online

Q: How do you feel about cyber security?

Statement:

“Staying secure online is important to me.”

63% of US and **60%** of UK citizens find staying secure online **very important.**



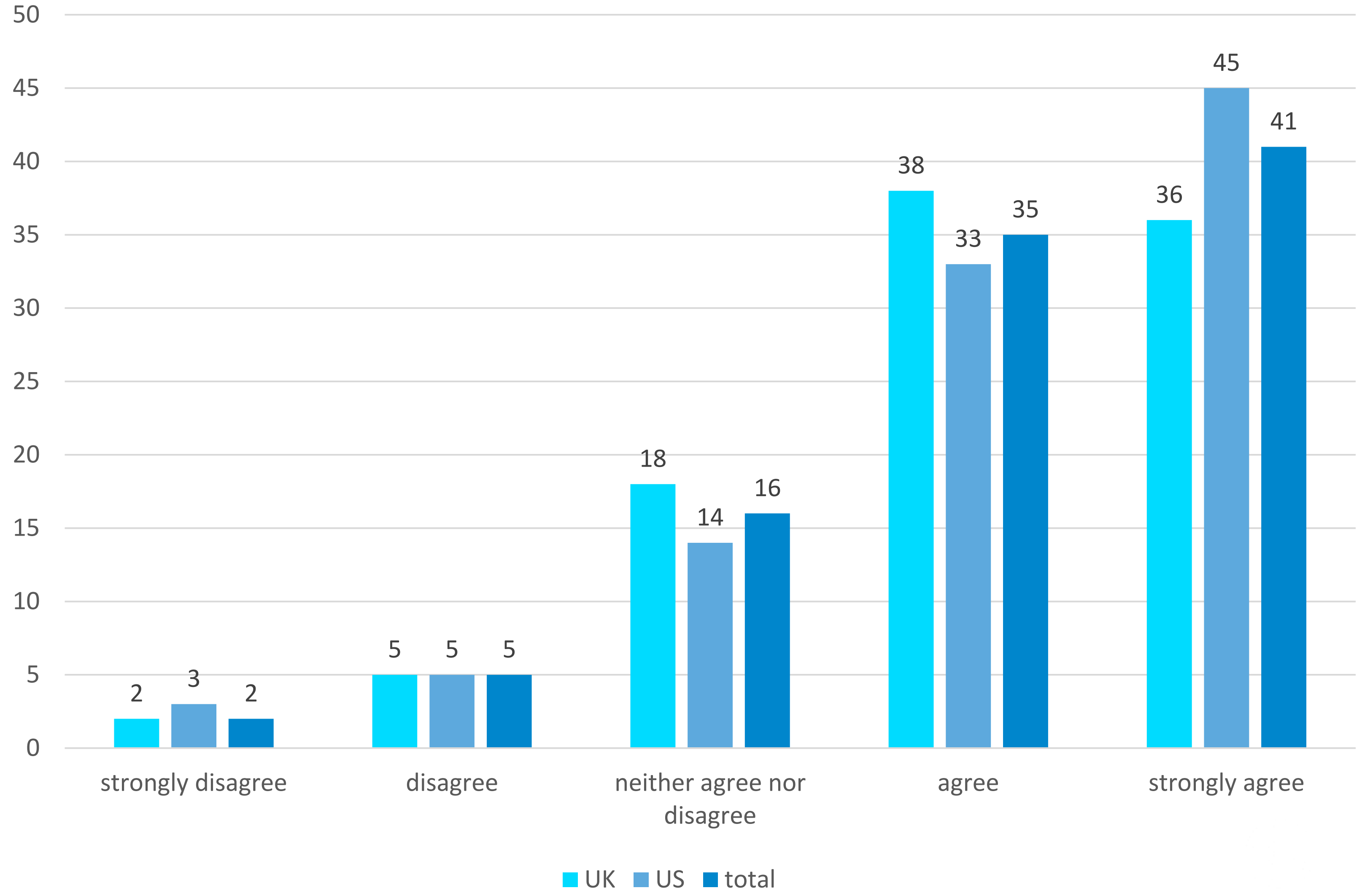
Prioritising online security

Q: How do you feel about cyber security?

Statement:

"I prioritise staying secure online."

45% of US citizens
36% of UK citizens
rated cyber security a
high priority for them.



Behaviors

Passwords

Q. What is your preferred method of remembering multiple passwords?

a. I write them down in a notebook **31%**

b. I store them in my phone or in my email **20%**

c. I just remember them (without writing them down) **26%**

d. I save passwords in the browser **11%**

e. I use a password manager application **12%**

Q. How often do you use different passwords for your important online accounts (e.g. emails, social media)?

a. Never
b. Rarely

47%

c. Sometimes

d. Very often
e. Always

20%

Q. I would use a password manager but…

a. I have heard that using the same password is risky, but never fully understood what the problem is **8%**

b. I understand what people are saying about the risks of using the same passwords for multiple accounts, but I don’t believe or care about it **7%**

c. I think it is worth using a password manager, but it is not a priority for me at the moment **18%**

d. I don’t think I can use a password manager because I don't think it is easy to use **7%**

e. I think using a password manager would get in the way of my productivity **6%**

f. I don’t trust any single provider with managing all my passwords **37%**

g. I don't know how to do it, even if I wanted to **14%**

Multi-Factor Authentication

Use of Multi-Factor Authentication (MFA)

48% of the participants had never heard of MFA.

Out of the 52% of the participants who had heard about it:

81% applied it at least once

90% of them reporting that they were still using MFA

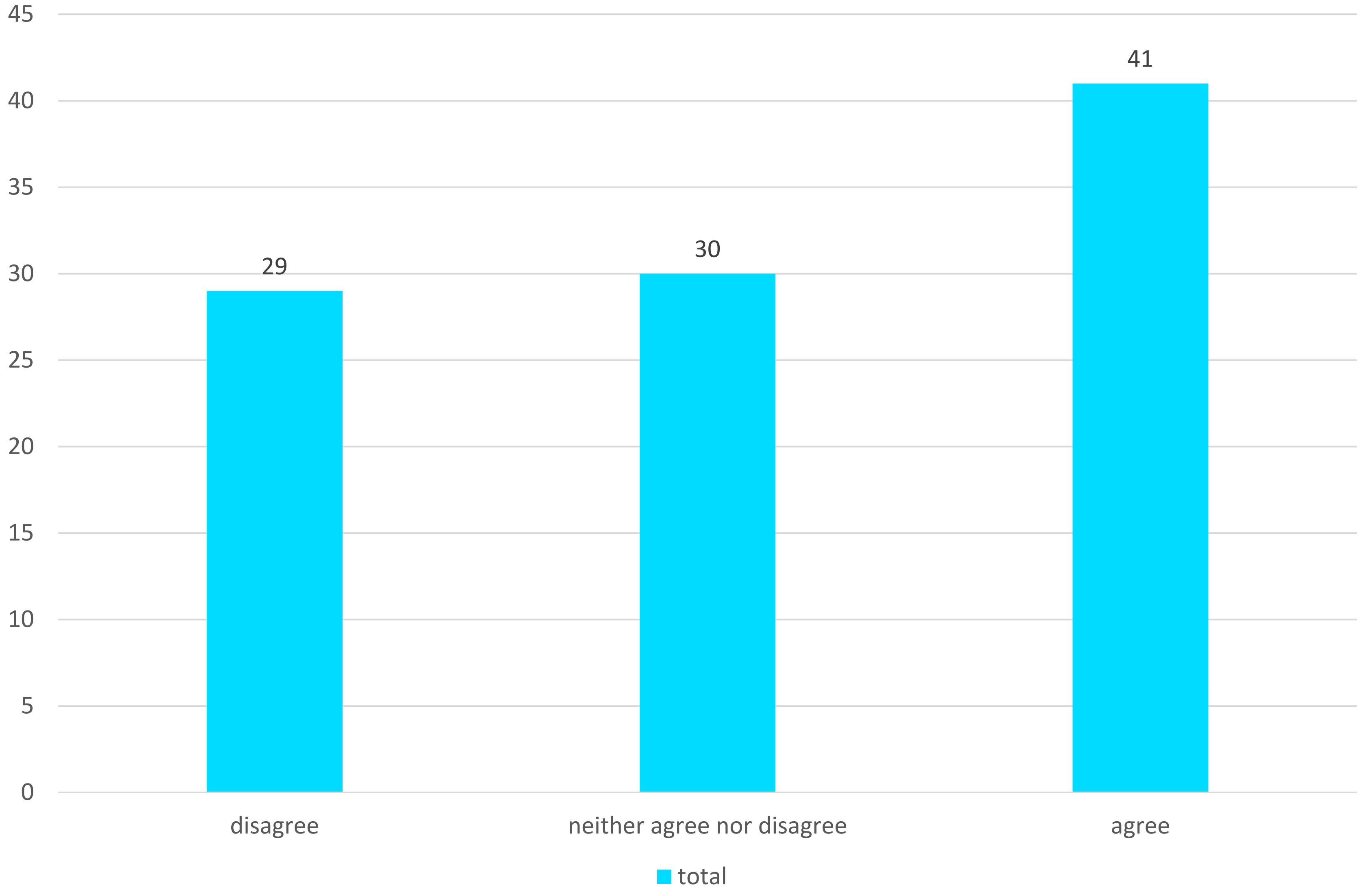
Feelings

Feelings of frustration

Q: How do you feel about cyber security?

Statement:

"I find staying secure frustrating."

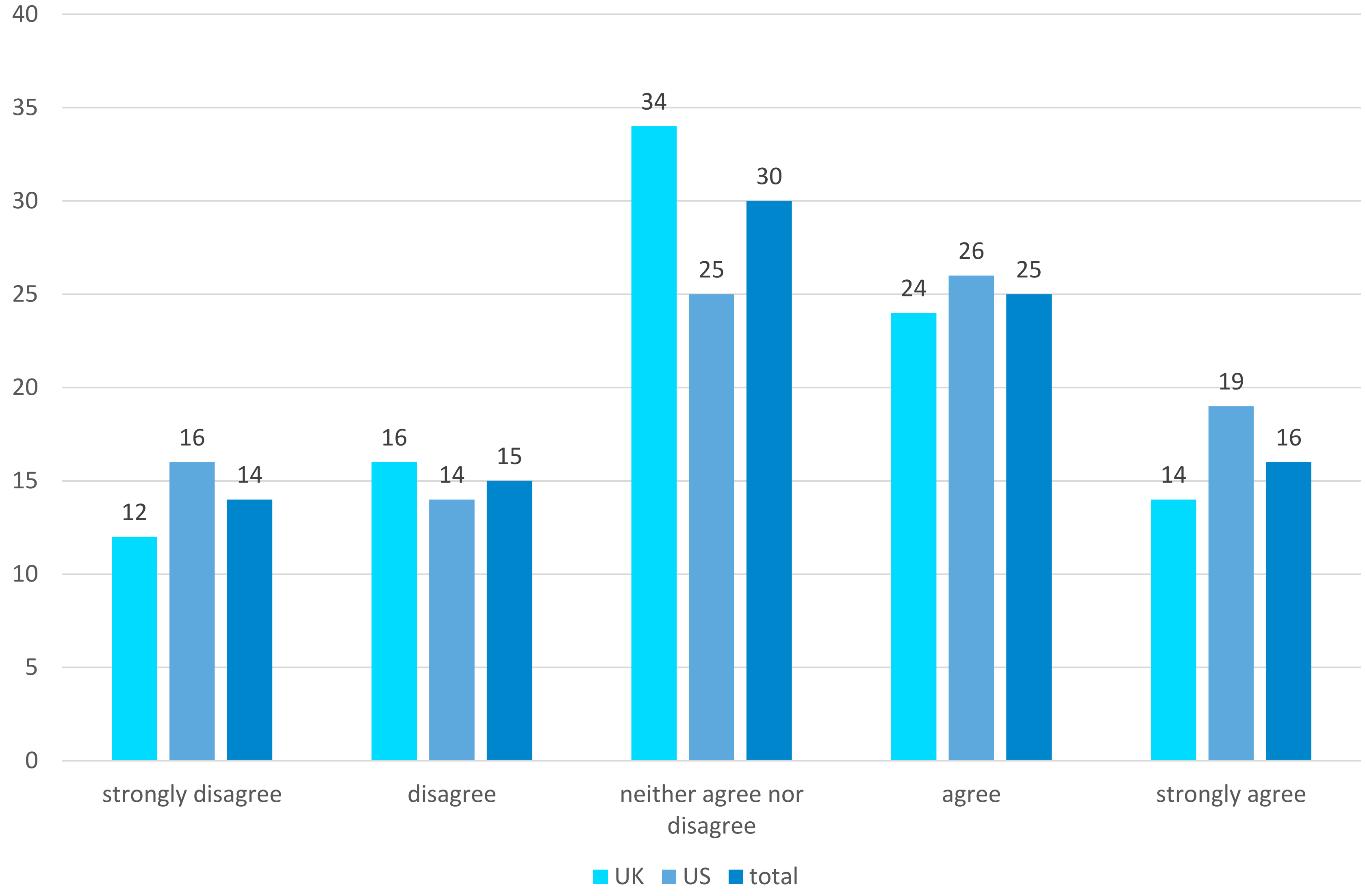


Feelings of intimidation

Q: How do you feel about cyber security?

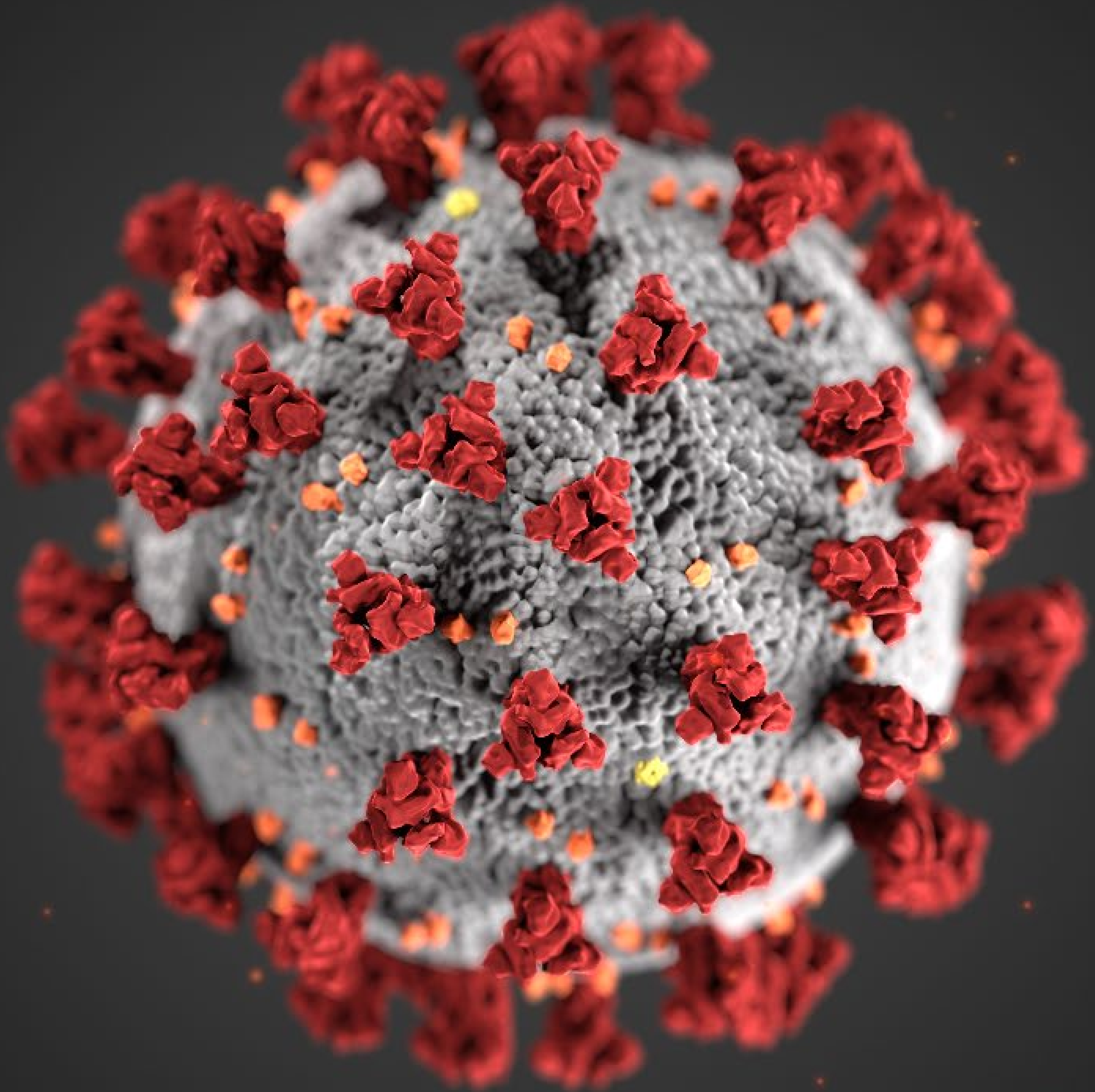
Statement:

"I find cyber security intimidating."



1010 1011 1100 1101
0010 0011 0100 0101
10000 10001 10010 1
1011 1100 1101 1110

1 0 0 1 0 1 0 1 0 1 0 1
0 1 0 1 1 1 0 1 0 1 0 0
1 0 1 0 0 1 0 1 0 1 1 1
0 1 0 1 1 0 1 0 1 0 0 1
HACKING DETECTED
RISK ALERT



Face Shield
18

#NoMoreHackersInHoodies

Peace of Mind

Focus on Behaviors

Phishing

Updates

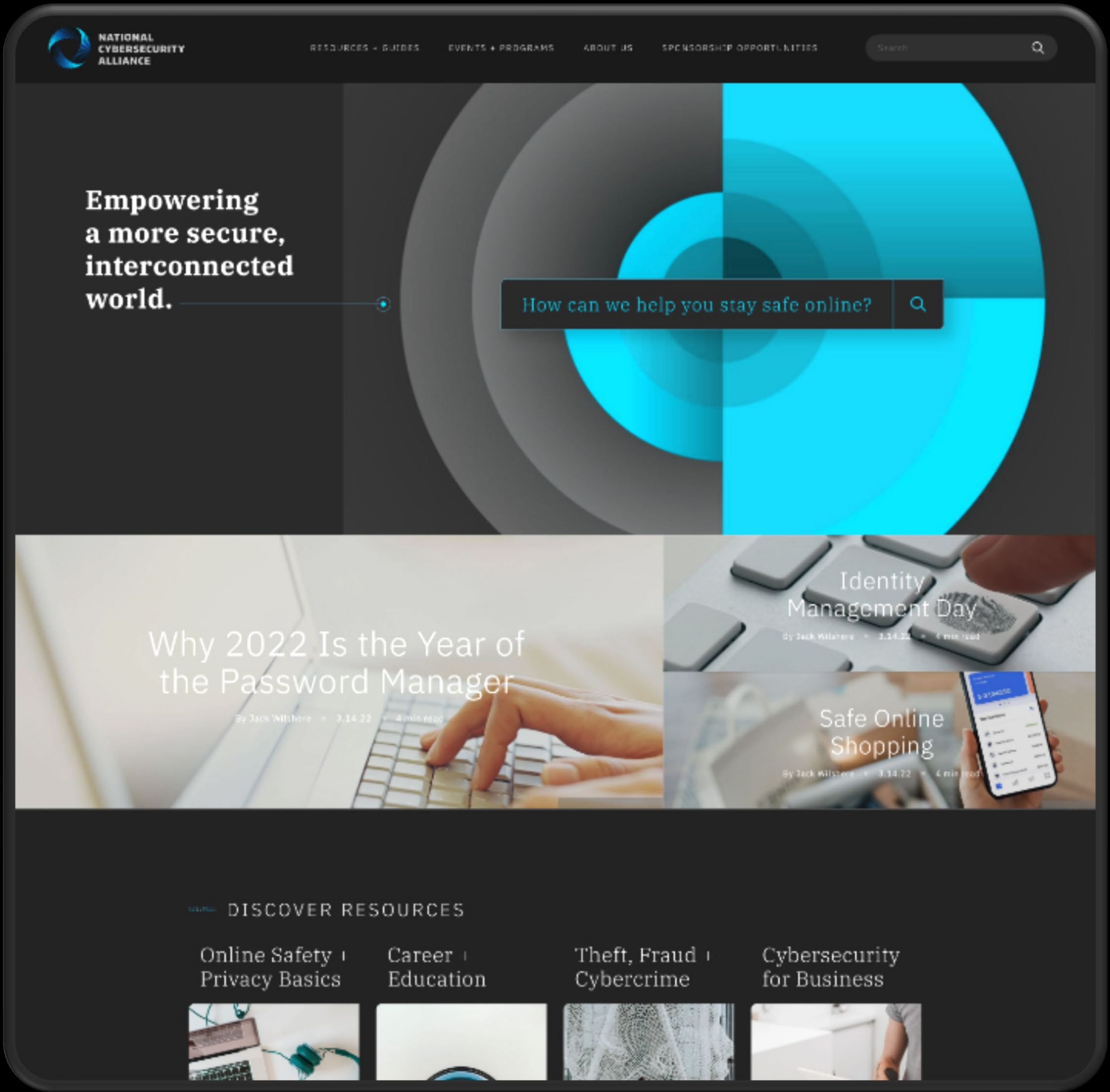
Passwords

MFA

Risk-based approach

Themes

It’s easy to stay safe online.



Empowering a more secure, interconnected world.

How can we help you stay safe online?

Why 2022 Is the Year of the Password Manager

By Jack Wilshere • 3.14.22 • 4 min read

Identity Management Day

By Jack Wilshere • 3.14.22 • 4 min read

Safe Online Shopping

By Jack Wilshere • 3.14.22 • 4 min read

DISCOVER RESOURCES

Online Safety Privacy Basics

Career Education

Theft, Fraud Cybercrime

Cybersecurity for Business

FEATURED PRESENTATION:

Review and Updates to NIST Cybersecurity Framework

○○○○

Kevin Stine

Chief, Applied Cybersecurity Division

National Institute of Standards and Technology

○○○○

NIST National Institute of Standards and Technology U.S. Department of Commerce

FISSEA Spring Forum
NIST Cybersecurity Framework

Kevin Stine, NIST
May 17, 2022

Celebrating our 50th Anniversary

The year 2022 marks **50 years** of NIST's cybersecurity research and the development of cybersecurity and privacy guidance.

Our work has helped better secure the state of technology that exists today—while providing the platform for the secure technology development of tomorrow.

Celebrate with us all year long!

- Website: nist.gov/cybersecurity/50th-anniversary-cybersecurity-nist (events, resources, and blogs all in one place!)
- Follow @NISTcyber on Twitter and use #NISTCyber50th
- Subscribe for our GovDelivery updates (use URL above)

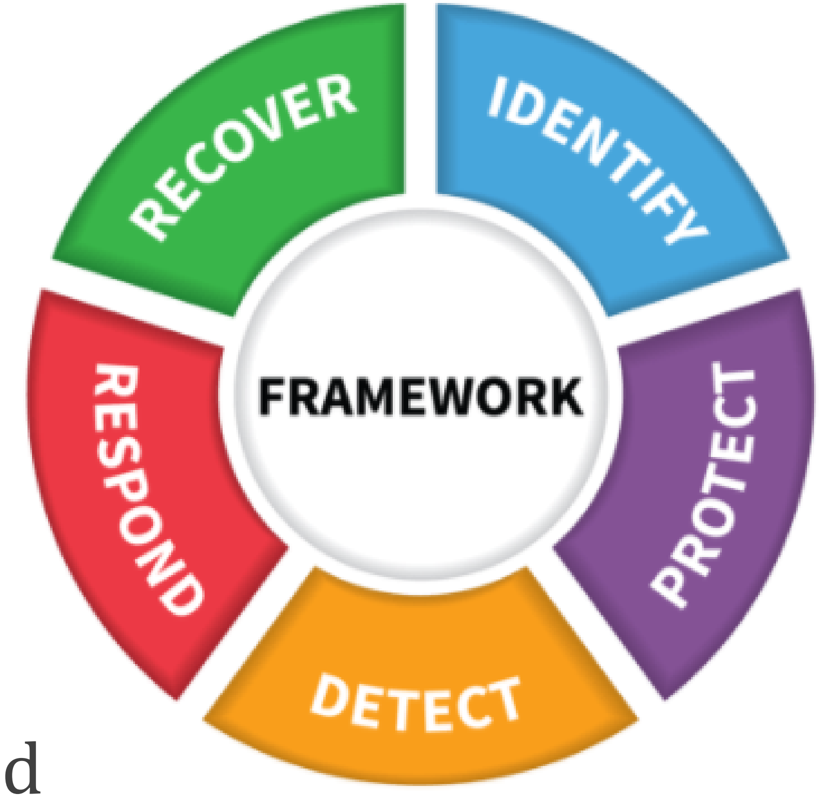
Cybersecurity Framework (CSF) History

- February 2013 – Executive Order 13636: Improving Critical Infrastructure Cybersecurity
- **February 2014 – CSF 1.0**
- December 2014 – Cybersecurity Enhancement Act of 2014 (P.L. 113-274)
- May 2017 – Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- **April 2018 – CSF. 1.1**
- April 2022 – NIST RFI on CSF Update Closed
- **Future – CSF 2.0**

Cybersecurity Framework (CSF)

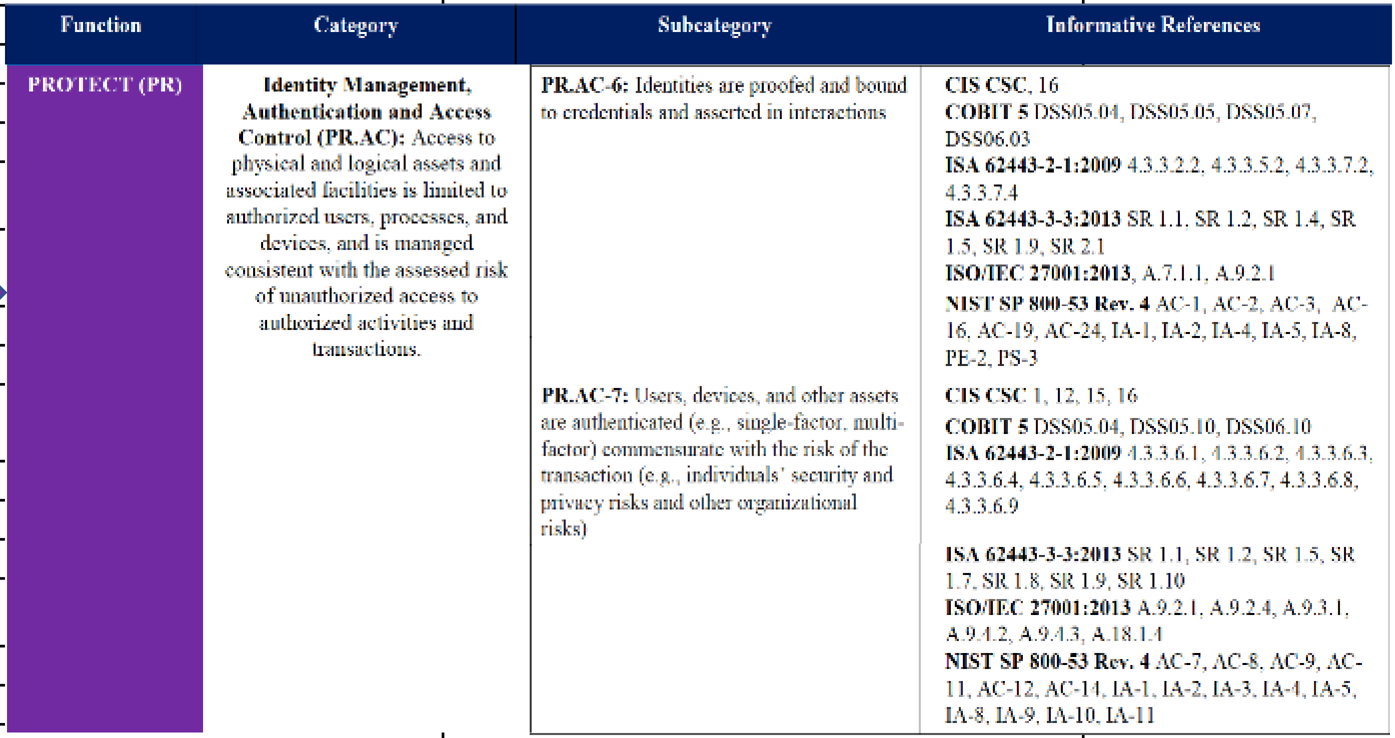
National Institute of Standards and Technology
U.S. Department of Commerce

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Guided by many perspectives – private sector, academia, public sector
- Align legal/regulatory requirements and organizational and risk management priorities



CSF Core

Function (5)	Category (23)	Subcategories (108)	Informative References
Identify (ID)	Asset Management		
	Business Environment		
	Governance		
	Risk Assessment		
	Risk Management Strategy		
	Supply Chain Risk Management		
Protect (PR)	Identity Management & Access Control		
	Awareness and Training		
	Data Security		
	Information Protection Processes and Procedures		
	Maintenance		
	Protective Technology		
Detect (DE)	Anomalies and Events		
	Security Continuous Monitoring		
	Detection Processes		
Respond (RS)	Response Planning		
	Communications		
	Analysis		
	Mitigation		
	Improvements		
Recover (RC)	Recovery Planning		
	Improvements		
	Communications		



Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

International Use

- Translated into Japanese, Spanish, Portuguese, Arabic, Bulgarian, Polish, Indonesian, French, Ukrainian
- Adapted into national cybersecurity policies, strategies, and requirements
- Use cases identified in all regions

Cybersecurity RFI on CSF 2.0

NIST is actively engaging stakeholders to solicit input on its cybersecurity resources

Cybersecurity Framework

Use of and potential updates to the NIST Cybersecurity Framework (CSF)

Cybersecurity Resources

Feedback on NIST cybersecurity resources, including relationship of the CSF with other NIST and other resources

Supply Chain Cybersecurity

The National Initiative for Improving Cybersecurity in Supply Chains

More info: https://www.nist.gov/cyberframework

Ways to Engage on CSF 2.0

Submit comments on our draft publications:
https://www.nist.gov/cyberframework/framework

Join our CSF workshops – stay tuned for that!
https://www.nist.gov/cybersecurity/cybersecurity-privacy-events

See us at other events/conferences:
https://www.nist.gov/cyberframework/events-and-presentations

National Institute of Standards and Technology
U.S. Department of Commerce

STAY IN TOUCH

CONTACT US

NIST.gov/cybersecurity

✉ Cybersecurity-Privacy@NIST.gov

@NISTcyber

FEATURED PRESENTATION:

Guide to Control Systems Cybersecurity

Keith Stouffer

Networked Control Systems Group Leader
Smart Connected Systems Division
Communications Technology Laboratory
National Institute of Standards and Technology

NIST Operational Technology (OT) Cybersecurity

FISSEA Spring Forum:
May 17, 2022

Keith Stouffer
Networked Control Systems Group Leader
Smart Connected Systems Division
Communications Technology Laboratory

National Institute of Standards and Technology
U.S. Department of Commerce

CTL Communications Technology Laboratory

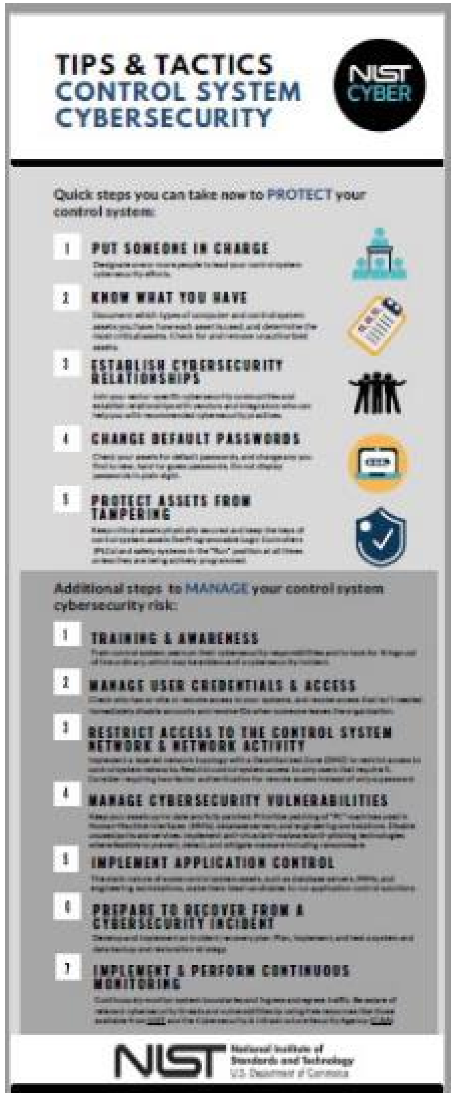
Operational Technology (OT) Definition

Operational technology (OT) encompasses a broad range of programmable systems or devices that **interact with the physical environment** (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems (ICS), building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.

NIST OT Cybersecurity Program

Cybersecurity risk management is an important factor to ensure the safe and reliable delivery of the goods and services provided and supported by OT. The NIST OT Security Program includes multiple collaborative projects from across the NIST Communications Technology Laboratory and Information Technology Laboratory.

https://csrc.nist.gov/projects/operational-technology-security



TIPS & TACTICS
CONTROL SYSTEM
CYBERSECURITY

NIST CYBER

Quick steps you can take now to PROTECT your control system:

1 PUT SOMEONE IN CHARGE

[illegible]

2 KNOW WHAT YOU HAVE

[illegible]

3 ESTABLISH CYBERSECURITY RELATIONSHIPS

[illegible]

4 CHANGE DEFAULT PASSWORDS

[illegible]

5 PROTECT ASSETS FROM TAMPERING

[illegible]

Additional steps to MANAGE your control system cybersecurity risk:

1 TRAINING & AWARENESS

[illegible]

2 MANAGE USER CREDENTIALS & ACCESS

[illegible]

3 RESTRICT ACCESS TO THE CONTROL SYSTEM NETWORK & NETWORK ACTIVITY

[illegible]

4 MANAGE CYBERSECURITY VULNERABILITIES

[illegible]

5 IMPLEMENT APPLICATION CONTROL

[illegible]

6 PREPARE TO RECOVER FROM A CYBERSECURITY INCIDENT

[illegible]

7 IMPLEMENT & PERFORM CONTINUOUS MONITORING

[illegible]

NIST National Institute of Standards and Technology U.S. Department of Commerce

Example OT Cybersecurity Resources

Manufacturing Extension Partnership Cybersecurity Resources

https://www.nist.gov/mep/cybersecurity-resources-manufacturers

Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide

https://csrc.nist.gov/news/2019/nistir-8183a-csf-mfg-profile-low-impact-level

National Cybersecurity Center of Excellence (NCCOE): Energy Sector, Healthcare Sector, Manufacturing Sector and Transportation Sector Projects

https://www.nccoe.nist.gov/

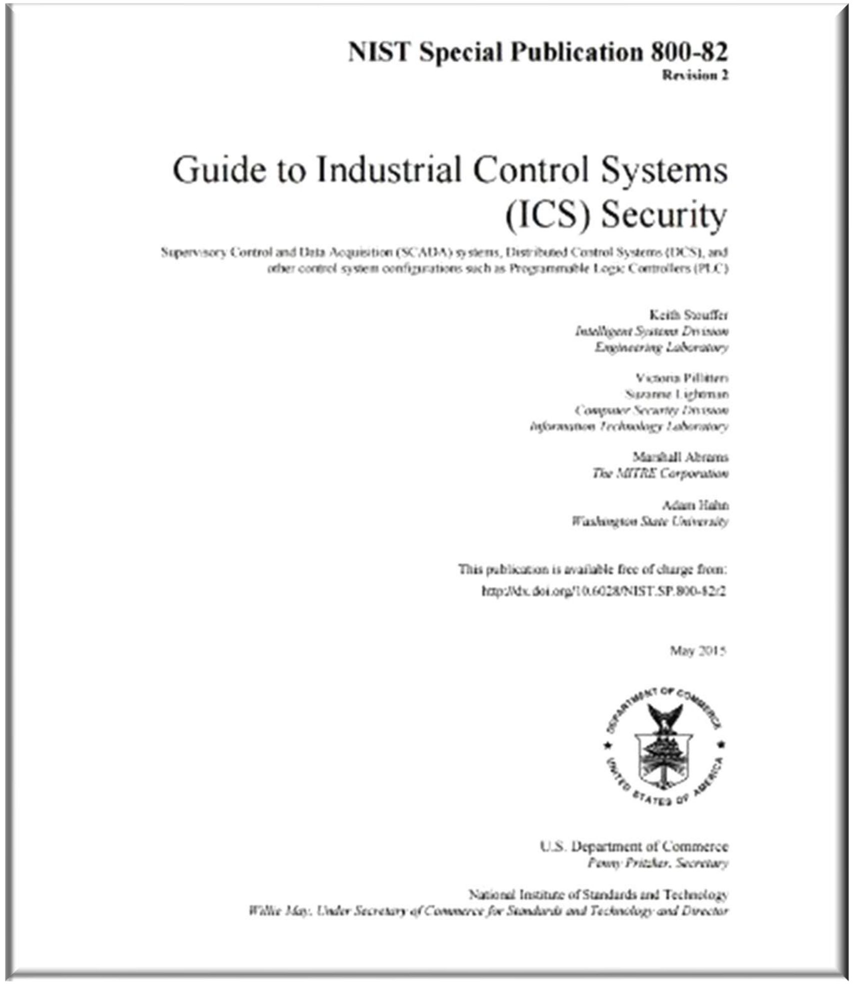
Cybersecurity & Infrastructure Security Agency (CISA) ICS Cybersecurity Recommended Practices

https://us-cert.cisa.gov/ics/Recommended-Practices

NIST Special Publication (SP) 800-82

Guide to Industrial Control Systems Security

- Provides a comprehensive cybersecurity approach for securing ICS, while addressing unique performance, reliability, and safety requirements, including implementation guidance for NIST SP 800-53 controls
- Initial draft - September 2006
- Revision 1 - May 2013
- Revision 2 - May 2015
- 3,000,000+ downloads, 1700+ citations, worldwide standard/guideline for industrial control system cybersecurity



NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems
(ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and
other control system configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Intelligent Systems Division
Engineering Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Marshall Abrams
The MITRE Corporation

Adam Hahn
Washington State University

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

May 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

NIST SP 800-82 Update

NIST has initiated an update of SP 800-82 to incorporate lessons learned over the past several years, to provide alignment to relevant NIST guidance, to provide alignment to other relevant control system cybersecurity standards and recommended practices, and to address changes in the threat landscape.

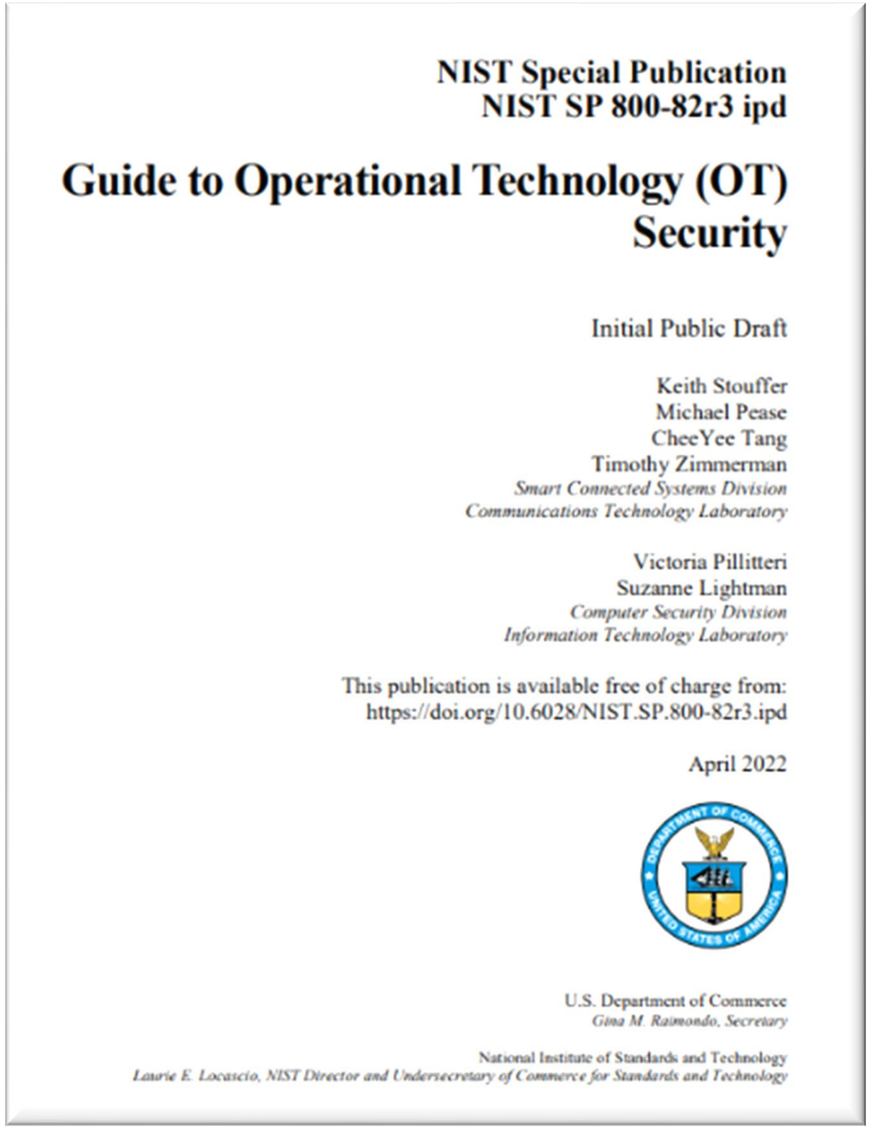
The initial public draft, which was published as SP 800-82, Revision 3, *Guide to Operational Technology (OT) Security* was released on April 26, 2022 and is open for public comment until July 1, 2022.

This initial public draft provides guidance on how to improve the security of OT systems while addressing their unique performance, reliability, and safety requirements.

NIST SP 800-82 Updates

- Expansion in scope from ICS to OT
- Updates to OT threats and vulnerabilities
- Updates to OT risk management, recommended practices, and architectures
- Updates to current activities in OT security
- Updates to security capabilities and tools for OT
- Additional alignment with other OT security standards and guidelines, including the Cybersecurity Framework (CSF)
- New tailoring guidance for NIST SP 800-53, Rev. 5 security controls
- An OT overlay for NIST SP 800-53, Rev. 5 security controls that provides tailored security control baselines for low-impact, moderate-impact, and high-impact OT systems.

https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft



NIST Special Publication
NIST SP 800-82r3 ipd

Guide to Operational Technology (OT) Security

Initial Public Draft

Keith Stouffer
Michael Pease
CheeYee Tang
Timothy Zimmerman
Smart Connected Systems Division
Communications Technology Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-82r3.ipd

April 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Undersecretary of Commerce for Standards and Technology

Example OT Cybersecurity Training and Certifications

CISA - Some courses available at no cost

https://us-cert.cisa.gov/ics/Training-Available-Through-ICS-CERT

International Society of Automation and International Electrotechnical Commission (ISA/IEC)

https://isaeurope.com/certification/

SANS

https://www.sans.org/cyber-security-courses/?focus-area=industrial-control-systems-security

Global Information Assurance Certification (GIAC)

https://www.giac.org/certifications/industrial-control-systems

SCADAhacker

https://scadahacker.com/training.html

FEATURED PRESENTATION: *Federal Training Opportunities for Control Systems Cybersecurity*

○○○○

Greg Bastien

Institutes Section Chief

Cyber Defense Education and Training

Cybersecurity and Infrastructure Security Agency

○○○○

CYBERSECURITY DEFENSE EDUCATION AND TRAINING (CDET)

INDUSTRIAL CONTROL SYSTEMS (ICS) CYBERSECURITY TRAINING

Greg Bastien
greg.bastien@cisa.dhs.gov

ICS Cybersecurity Training

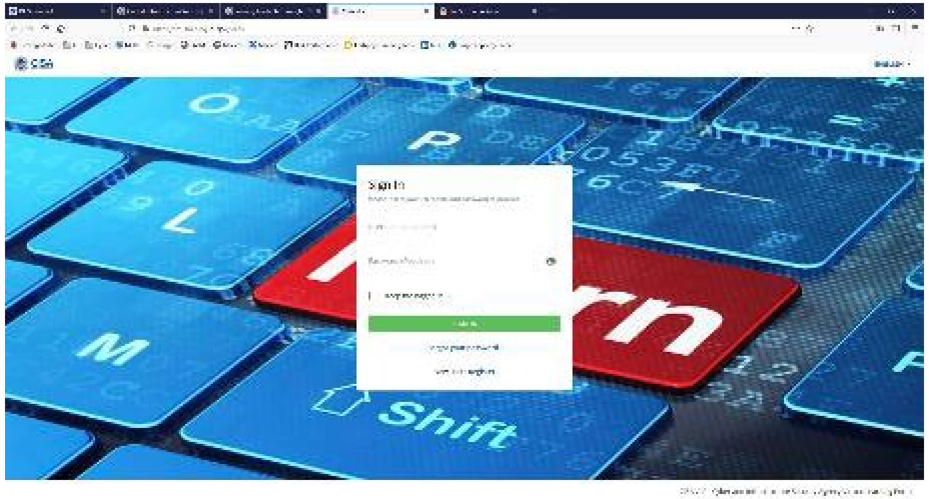
ICS Cybersecurity Training falls into one of four categories:

1. The Virtual Learning Portal
2. ICS301V and ICS401V Online Training
3. Instructor-led, in-class Training
4. Regional Training

https://www.cisa.gov/uscert/ics/Training-Available-Through-CISA

ICS Cybersecurity Training

1. **The Virtual Learning Portal (VLP)** https://ics-training.inl.gov/learn
   - Students register for their own VLP Account
   - Students can take the training at their leisure
   - There are currently 13 courses available
     - Operational Security (OPSEC) for Control Systems (100W) - 1 hour
     - Differences in Deployments of ICS (210W-1) – 1.5 hours
     - Influence of Common IT Components on ICS (210W-2) – 1.5 hours
     - Common ICS Components (210W-3) – 1.5 hours
     - Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
     - Cybersecurity Risk (210W-5) – 1.5 hours
     - Current Trends (Threat) (210W-6) – 1.5 hours
     - Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
     - Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
     - Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
     - Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10) – 1.5 hours
     - Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11) – 1.5 hours
     - ICS Cybersecurity Landscape for Managers (FRE2115)



ICS Cybersecurity Training

2. ICS301V and ICS401V Online Training

- Courses start every other Monday (alternating)
- Students must register for each individual course
- Students must complete the training within the allotted timeline
- The 301V and 401V courses are a prerequisite for attending the 301L and 401L in-class training

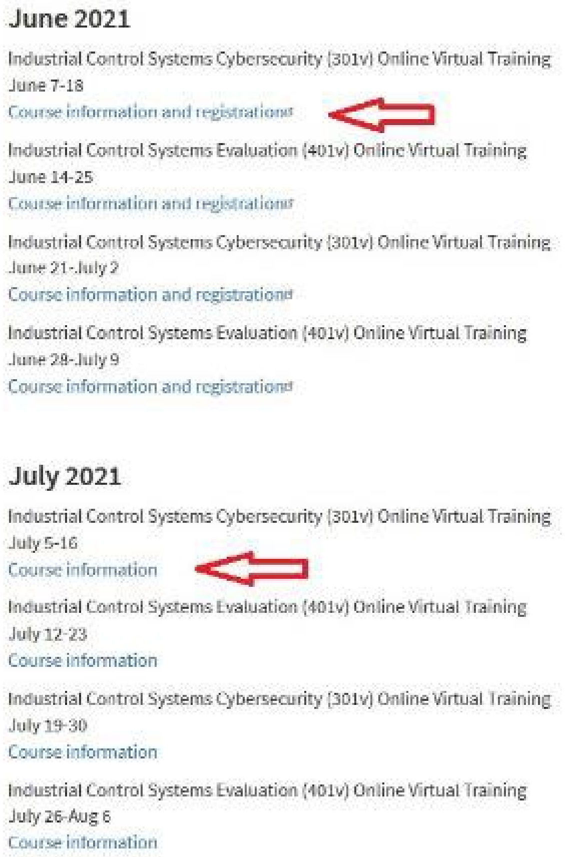
ICS Cybersecurity (301V)
This course provides an online virtual training based on understanding, protecting, and securing Industrial Control Systems (ICS) from cyber-attacks. In order to understand how to defend IT and OT systems, trainees will learn about common cyber vulnerabilities and the importance of understanding the environment they are tasked to protect. Learning the weaknesses of systems will enable trainees to identify mitigation strategies, policies, and programs that will provide the defense-in-depth needed to ensure a more secure ICS environment.

ICS Evaluation (401V)
This course provides online training on how to analyze, evaluate, and document the cybersecurity posture of an organization's Industrial Control Systems (ICS) for the purpose of identifying recommended changes. Specifically, the course will utilize a multi-step repeatable process, within a simulated ICS environment, that teaches how to analyze cybersecurity weaknesses and threats, evaluate and map findings, document potential mitigations, and provide ongoing resolutions to strengthen the cybersecurity posture.

ICS Cybersecurity Training

2. ICS301V and ICS401V Online Training

How do I register? https://www.cisa.gov/uscert/ics/Calendar



June 2021

Industrial Control Systems Cybersecurity (301v) Online Virtual Training
June 7-18
Course information and registration

Industrial Control Systems Evaluation (401v) Online Virtual Training
June 14-25
Course information and registration

Industrial Control Systems Cybersecurity (301v) Online Virtual Training
June 21-July 2
Course information and registration

Industrial Control Systems Evaluation (401v) Online Virtual Training
June 28-July 9
Course information and registration

July 2021

Industrial Control Systems Cybersecurity (301v) Online Virtual Training
July 5-16
Course information

Industrial Control Systems Evaluation (401v) Online Virtual Training
July 12-23
Course information

Industrial Control Systems Cybersecurity (301v) Online Virtual Training
July 19-30
Course information

Industrial Control Systems Evaluation (401v) Online Virtual Training
July 26-Aug 6
Course information

ICS Cybersecurity Training

3. Instructor-led, in-class Training (301L and 401L)

a. Courses taught at the Idaho National Laboratory [INL] (Idaho Falls, ID)
b. These facilities are currently closed due to COVID19
c. The course schedule will be posted 90 days prior https://www.cisa.gov/uscert/ics/Calendar
d. Students must register and be approved for the training. (seating is very limited)
e. The 301V and 401V courses are a prerequisite for the 301L and 401L course

ICS Cybersecurity Lab (301L) - 5 days
This is the companion and follow-on course to the 301V. This course provides hands-on training on understanding, protecting, and securing Industrial Control Systems (ICS) from cyber-attacks and includes a Red versus Blue team exercise conducted within an actual Control Systems environment. Attendees will get an instructor-led hands-on experience with opensource operating systems and security tools such as Kali Linux and Security Onion. In addition, the training provides the opportunity to network and collaborate with other colleagues involved in operating and protecting Control System networks.

ICS Evaluation (401) - 5 days
This instructor-led 5-day course provides hands-on training on how to analyze, evaluate, and document the cybersecurity posture of an organization’s Industrial Control Systems (ICS) for the purpose of identifying recommended changes. Specifically, the course will utilize a multi-step repeatable process, within a simulated ICS environment, that teaches how to analyze cybersecurity weaknesses and threats, evaluate and map findings, document potential mitigations, and provide ongoing resolutions to strengthen the cybersecurity posture.

ICS Cybersecurity Training

4. Regional Training

- Training provided virtually or in-person by INL personnel
- Training consists to 100 and 200 level courses, CyberStrike and CyberCHAMP
- Regional events are scheduled through the Regional CSA or PSA
- We are working to virtualize the 100 and 200 level training

Introduction to Control Systems Cybersecurity (101)
This course introduces students to the basics of Industrial Control Systems (ICS) cybersecurity. This includes a comparative analysis of IT and ICS architectures, understanding risk in terms of consequence, security vulnerabilities within ICS environments, and effective cyber risk mitigation strategies for the Control System domain.

Intermediate Cybersecurity for Industrial Control Systems (201) Part 1
This course builds on the concepts learned in the Introduction to ICS Cybersecurity (101) course. This course provides technical instruction on the protection of Industrial Control Systems using offensive and defensive methods. Attendees will recognize how cyber attacks are launched, why they work, and mitigation strategies to increase the cybersecurity posture of their Control System networks. In addition, this course acts as a prerequisite for the next course, Intermediate Cybersecurity for Industrial Control Systems (202), which offers hands-on application of concepts presented.

Intermediate Cybersecurity for Industrial Control Systems (202) Part 2
This hands-on course is structured to help students recognize how attacks against Process Control Systems can be launched, why they work, and provides mitigation strategies to increase the cyber security posture of their Control Systems networks.

CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

BREAK

Federal Information Security Educators (FISSEA) Spring Forum

The Forum will resume at 2:30pm ET

fissea
FEDERAL
CYBERSECURITY | INNOVATION AWARENESS TRAINING

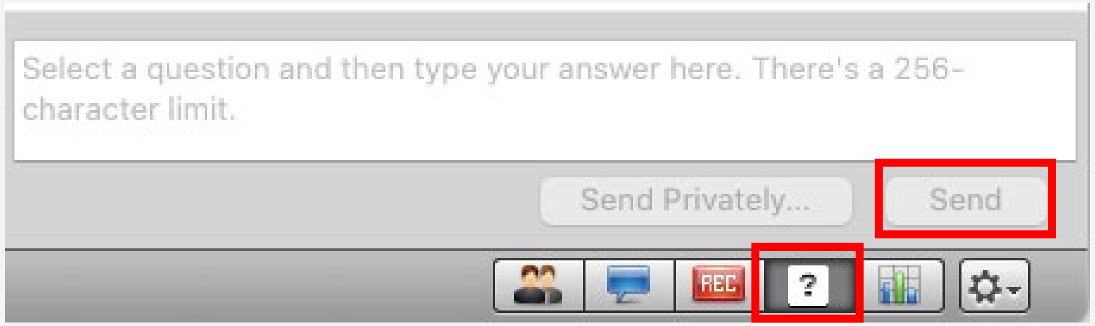
#FISSEA2022

NIST.GOV/FISSEA

LOOKING FORWARD

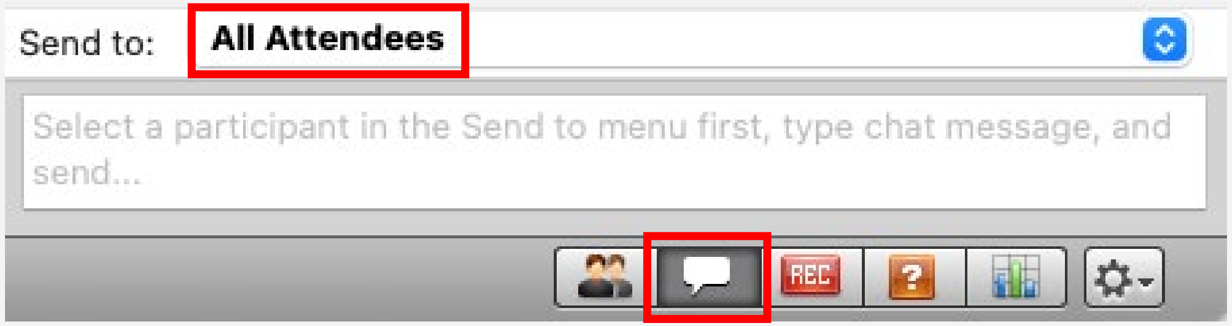
ENGAGE DURING THE EVENT

- **Please use the Q&A to send questions for the speakers**. Be sure to click the "send" button after typing your question. We will do our best to answer all questions.



Select a question and then type your answer here. There's a 256-character limit.

- **Please use the CHAT to make comments and share information** with other attendees. Please remember to not use the chat space for promoting any commercial products or services.



Send to: All Attendees

Select a participant in the Send to menu first, type chat message, and send...

INNOVATOR OF THE YEAR AWARD RECOGNITION AND FIRESIDE CHAT

Menachem Goldstein

Moderator
Cybersecurity Specialist
Enterprise Cybersecurity Department
Pension Benefit Guaranty Corporation

Deborah Coleman

2020 Award Recipient
Cybersecurity Awareness and Training
Program Manager
U.S. Department of Education

FISSEA

Innovator of the Year Award

Honorable Mention

Dr. Loyce Pailen

Congratulations!

Dr. Loyce Pailen

- Director, UMGC Center for Security Studies
- Teaching all ages: K-12, university & beyond.
- Some Accomplishments:
  - Doctoral degree
  - CISSP
  - 6 Children's Books

Prior Innovator of the Year

Deborah Coleman

Current Innovator of the Year

Kimberly Mentzell

Kimberly Mentzell

- Director of Cybersecurity and Aerospace, Maryland Department of Commerce
- Professor, Community Volunteer
- Some Accomplishments:
  - Established Maryland’s K-12 Cyber Range
  - Co-led the UMGC 2022 Gen Cyber Teacher Camp

Fireside Chat

or maybe

A little about yourself.

Favorite part of your job?

Tailoring training for children.

New times: new approaches?

Current Events: Training Changes

Training for non-techies

Beyond the Annual Training

Our biggest challenge?

Message for the Audience

Congratulations!

INDIVIDUALIZED AWARENESS WHILE ENSURING COMPLIANCE

Carolyn Schmidt

Team Lead

Office of Information Systems Management

National Institute of Standards and Technology

Individualized Awareness While Ensuring Compliance

Carolyn Schmidt, Team Lead

FISSEA Spring Forum

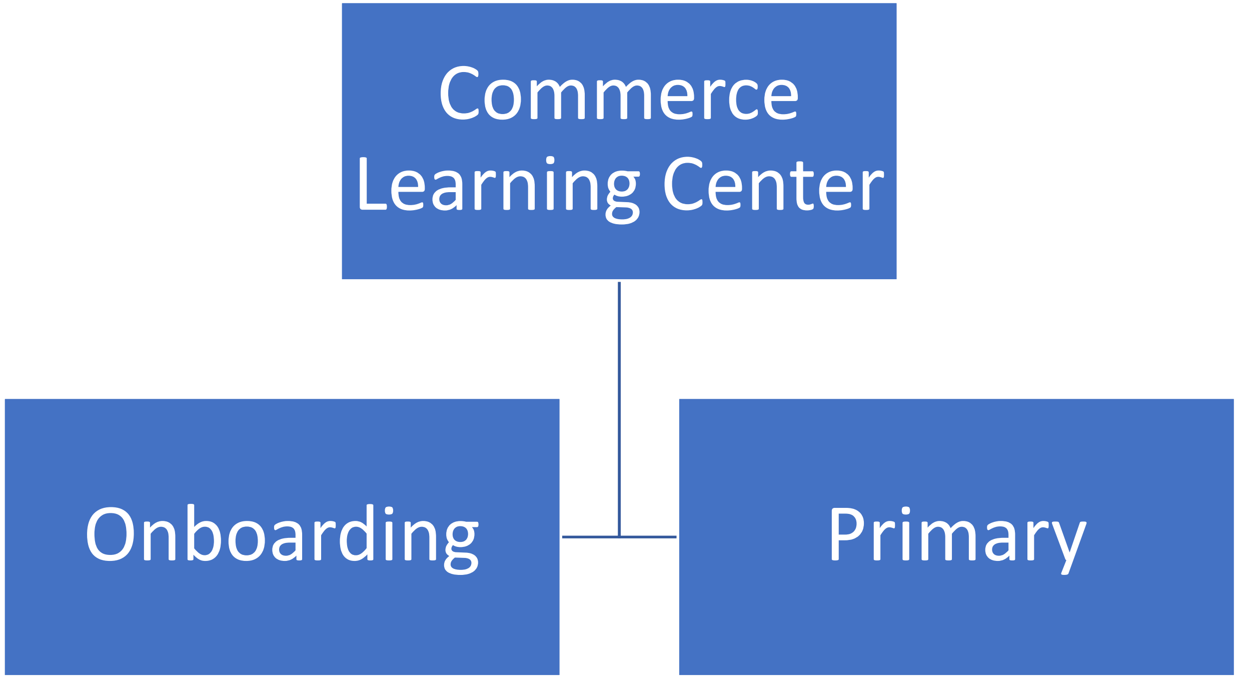
May 17, 2022

IT Security and Privacy General Awareness training

- Infrastructure
- Content **
- Compliance

infrastructure

Transcript data is merged from Onboarding to Primary, and thereafter deactivated



New staff (incoming)

Accounts are self-registration

Existing staff (federal and associates)

Accounts are based on issuance of IT access

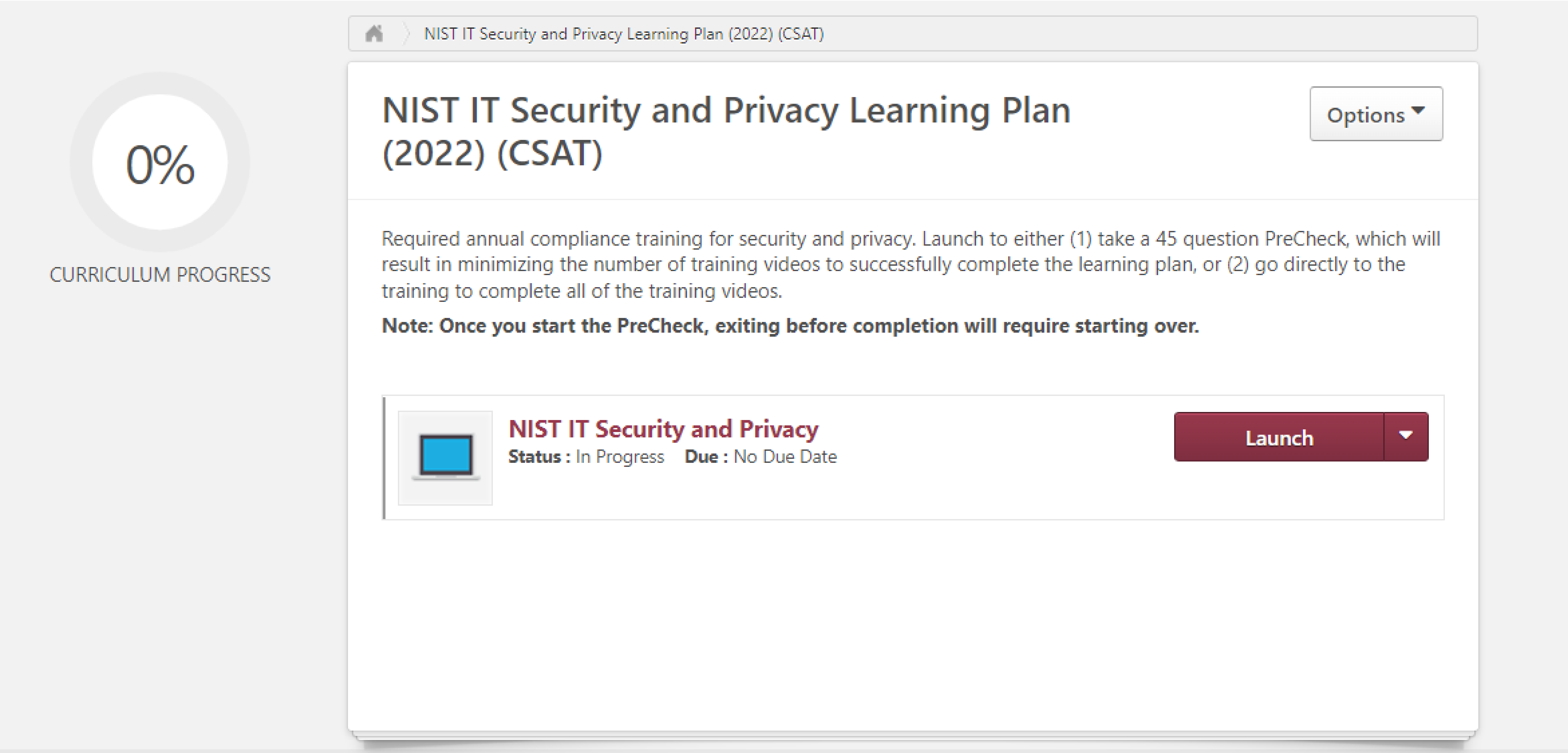
content

New Users	Existing Users
Static	Dynamic
Introductory	Customized based on routine requirements, threat environment, and current issues (e.g., CUI, PII, privacy, Insider Threat, etc.)

Problem Space

(content challenges)

- Maintenance
- Cost
- Relevance
- Interest



NIST IT Security and Privacy Learning Plan (2022) (CSAT)

0%

CURRICULUM PROGRESS

NIST IT Security and Privacy Learning Plan (2022) (CSAT)

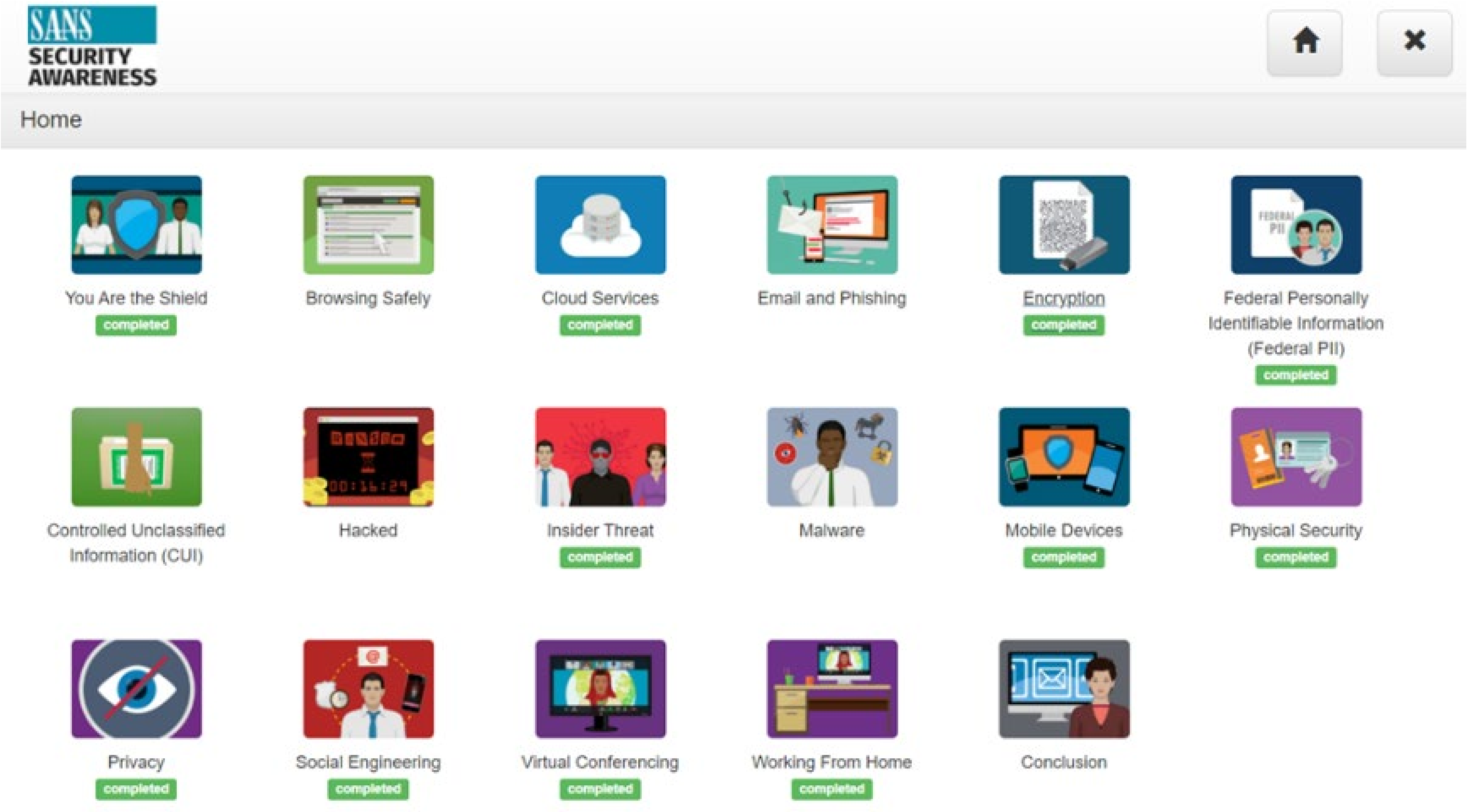
Required annual compliance training for security and privacy. Launch to either (1) take a 45 question PreCheck, which will result in minimizing the number of training videos to successfully complete the learning plan, or (2) go directly to the training to complete all of the training videos.

Note: Once you start the PreCheck, exiting before completion will require starting over.

NIST IT Security and Privacy

Status : In Progress **Due :** No Due Date

Individualized Learning



You Are the Shield
completed

Browsing Safely

Cloud Services
completed

Email and Phishing

Encryption
completed

Federal Personally Identifiable Information (Federal PII)
completed

Controlled Unclassified Information (CUI)

Hacked

Insider Threat
completed

Malware

Mobile Devices
completed

Physical Security
completed

Privacy
completed

Social Engineering
completed

Virtual Conferencing
completed

Working From Home
completed

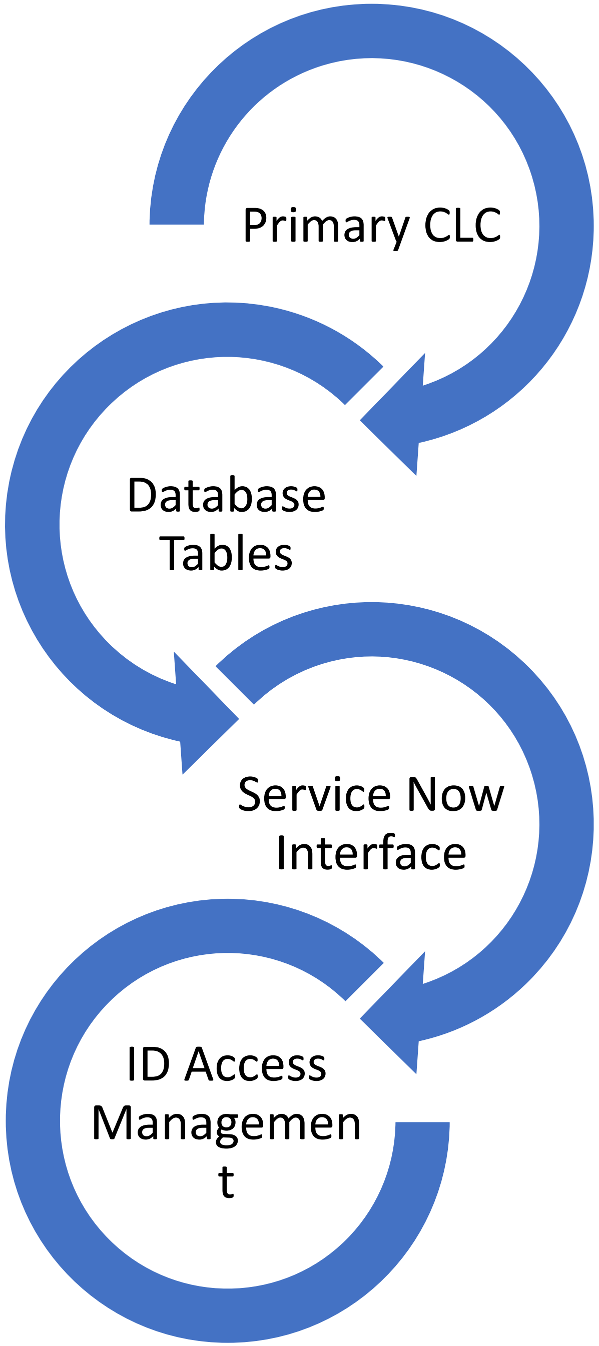
Conclusion

45-question
PreCheck assessment

3 questions per video
(excludes intro/conclusion)

The example shows a user was only required to view 6 of the 17 videos (as indicated by the Completed status below each) based on their knowledge in the various topic areas.

Compliance



Primary CLC

Database Tables

Service Now Interface

ID Access Managemen t

?

(e) Carolyn.Schmidt@nist.gov
(o) 301-975-3243

FEDERAL CYBERSECURITY ROLE-BASED TRAINING STUDY

Julie Haney

Usable Cybersecurity Program Lead
Visualization & Usability Group
National Institute of Standards and Technology

Jody Jacobs

Usable Cybersecurity
Visualization & Usability Group
National Institute of Standards and Technology

NIST Cybersecurity Role-Based Training Study

Jody Jacobs, Julie Haney, and Susanne Furman
National Institute of Standards and Technology

May 2022

National Institute of Standards and Technology
U.S. Department of Commerce

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Study Overview

Purpose: To better understand the needs, challenges, and approaches of federal cybersecurity role-based training (RBT) activities

Focus Groups

8 focus groups of feds **(n=29)** working in departments, sub-component agencies in departments, and independent agencies

Online, Anonymous Survey

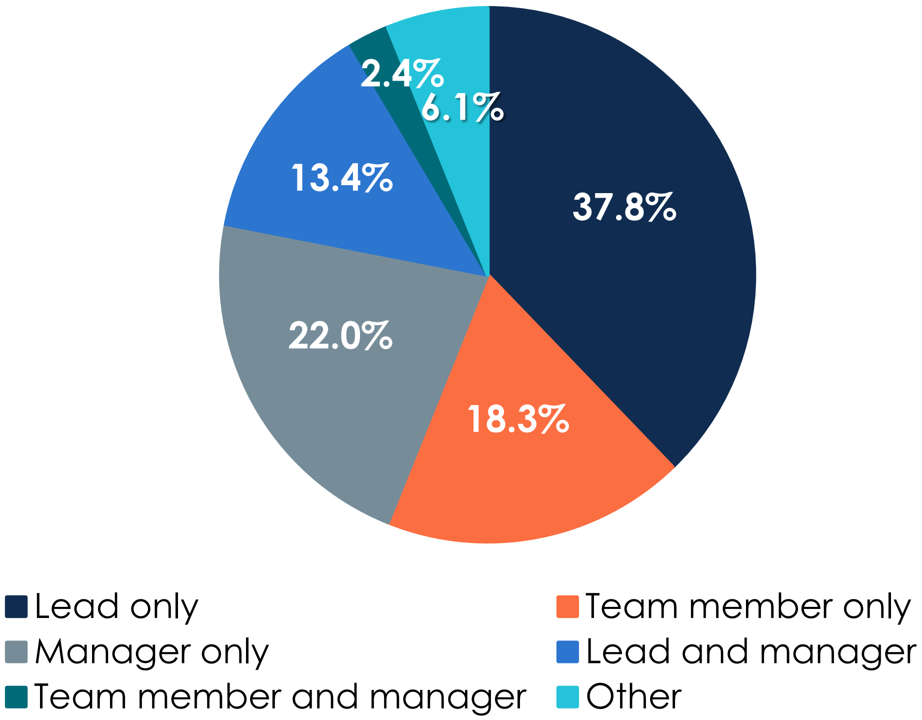
Survey of a broader population **(n=82)** of feds who are responsible for implementing or overseeing RBT activities

Study results are informing the revision of NIST SP 800-50 and 800-16 and can serve as a resource for those implementing or overseeing RBT activities.

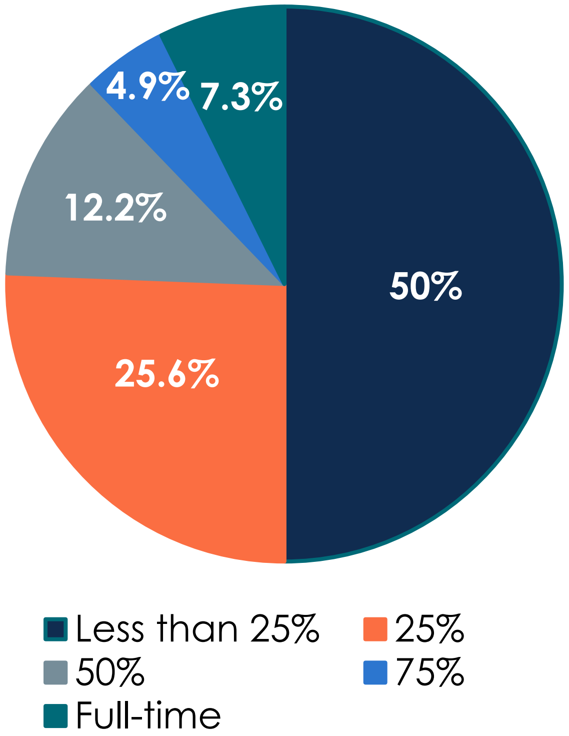
Who took the survey

RBT Involvement

RBT Roles



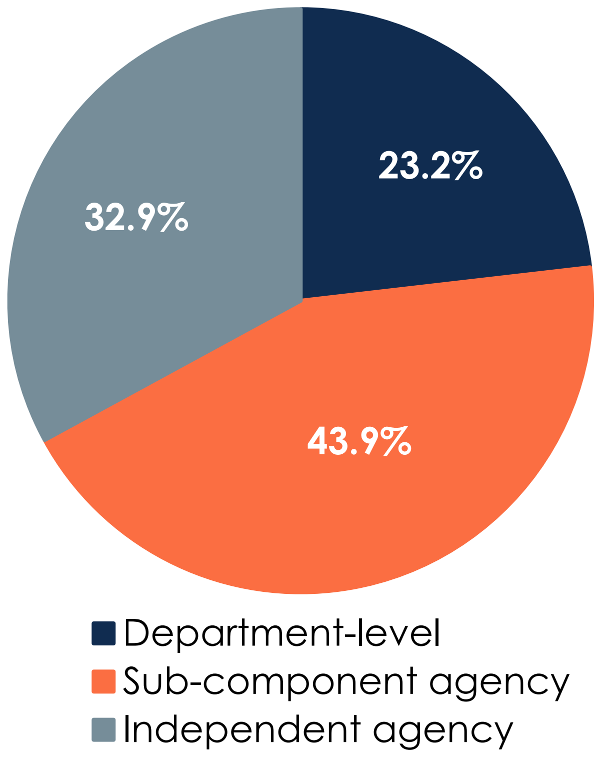
% of Time Spent on RBT



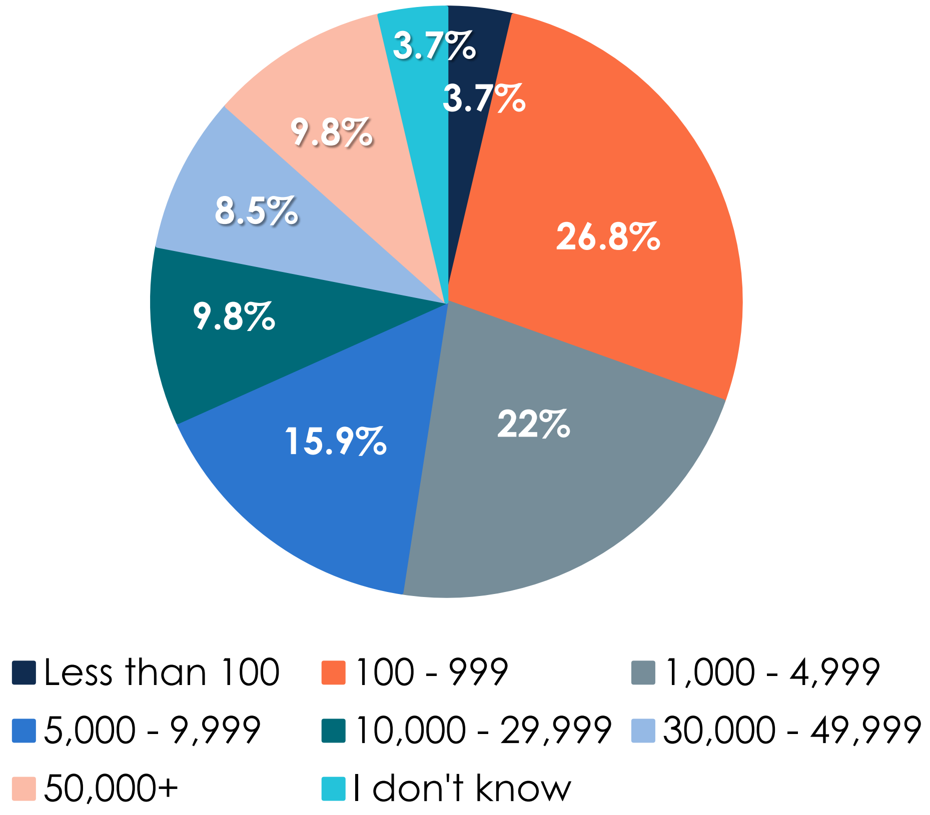
60% had more than 5 years of experience with RBT

Represented Organizations

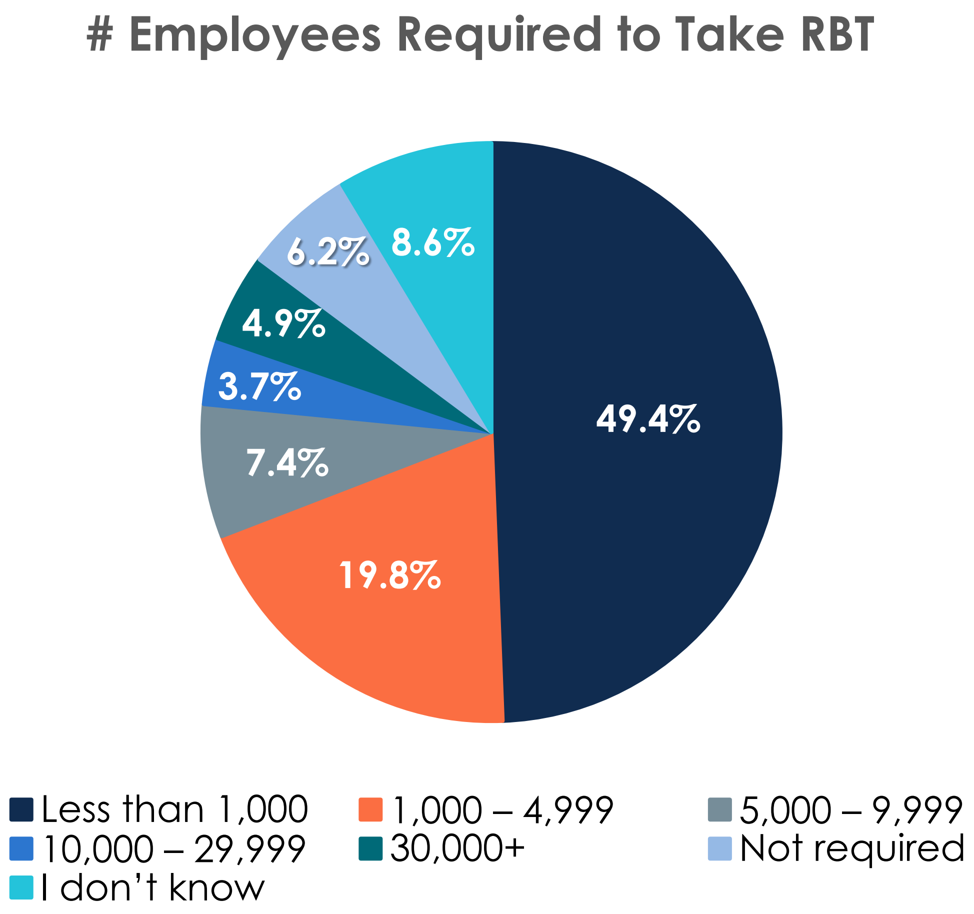
Organization Type

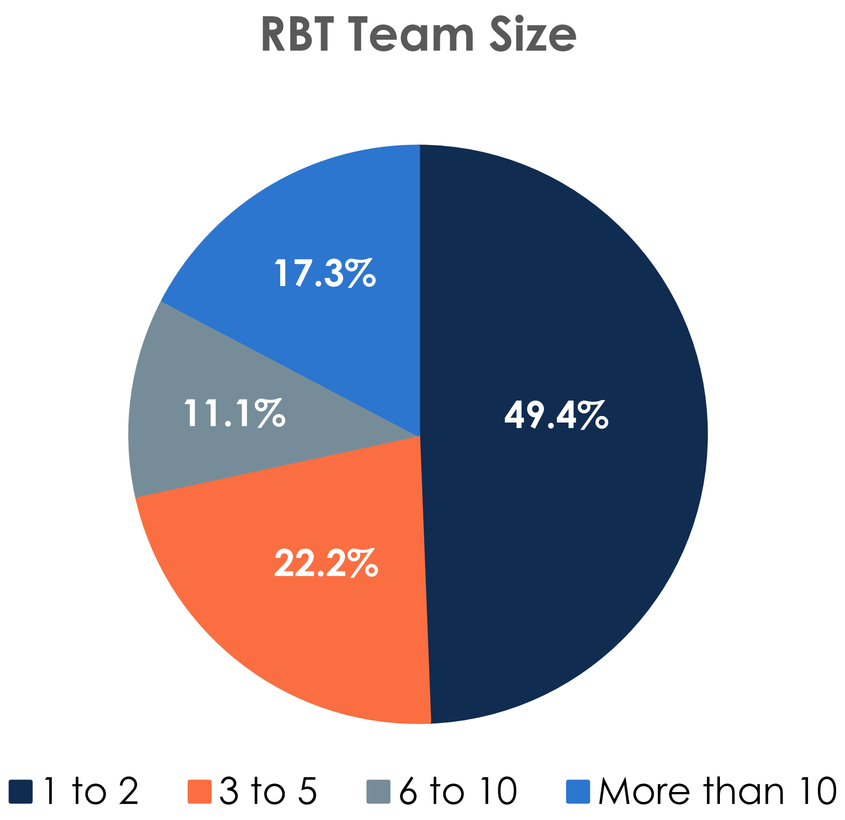


Organization Size (# federal employees)



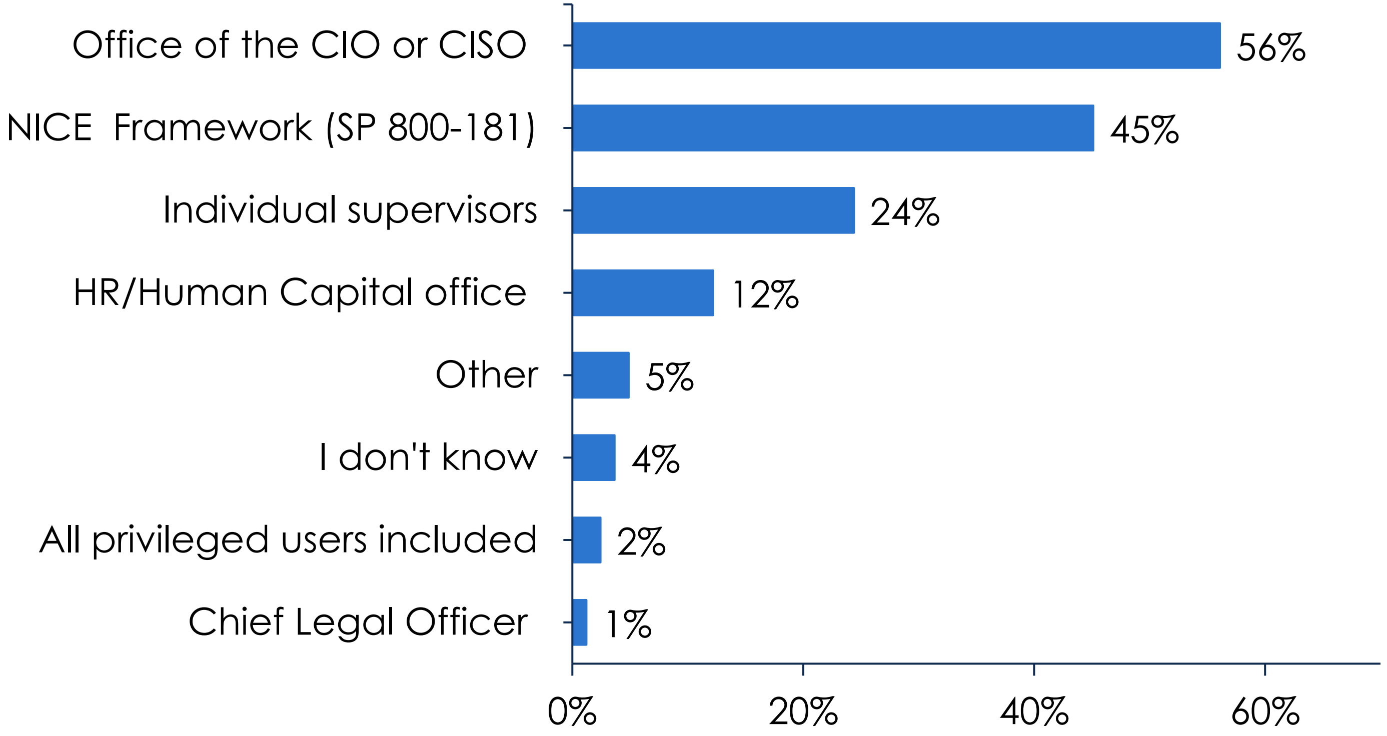
Represented RBT Activities





What we found

RBT Assignment Responsibility

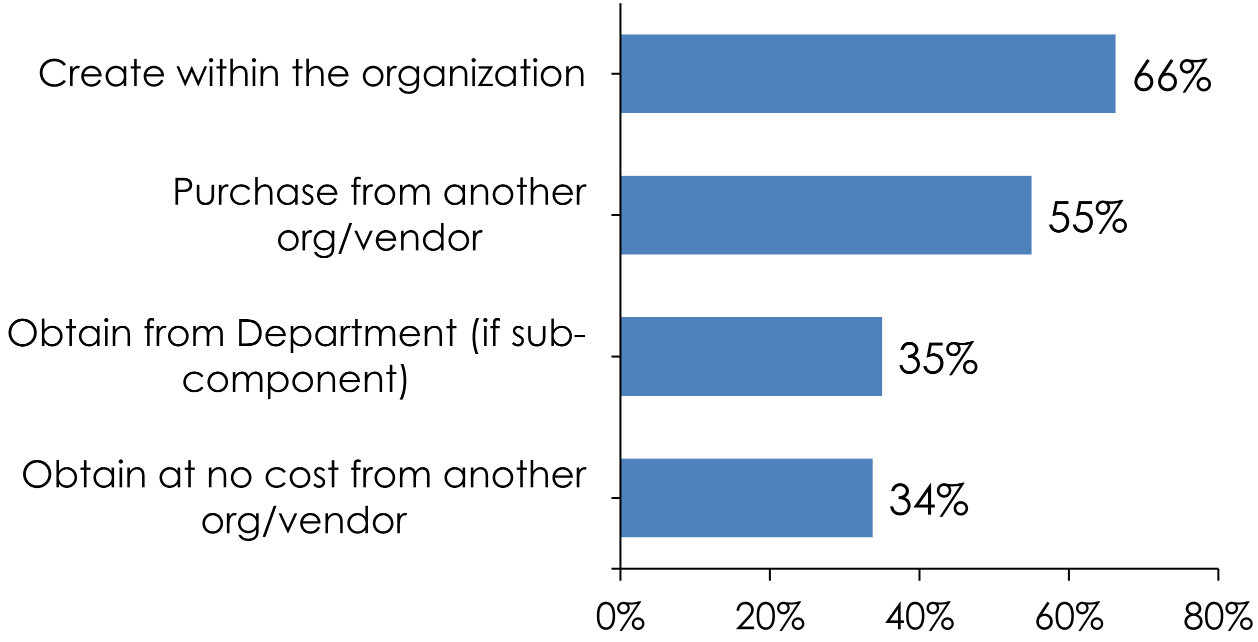


How organizations determine which employees take RBT (select all that apply)

26%: Identifying which employees need to take RBT is moderately/very challenging

"We need our human resources management system to be upgraded to more accurately track the job roles so that we can automatically align the job roles with the NIST framework and automatically assign role-based trainings to the users." (Q53)

RBT Content, Materials, and Guidance



How organizations obtain RBT content (select all that apply)

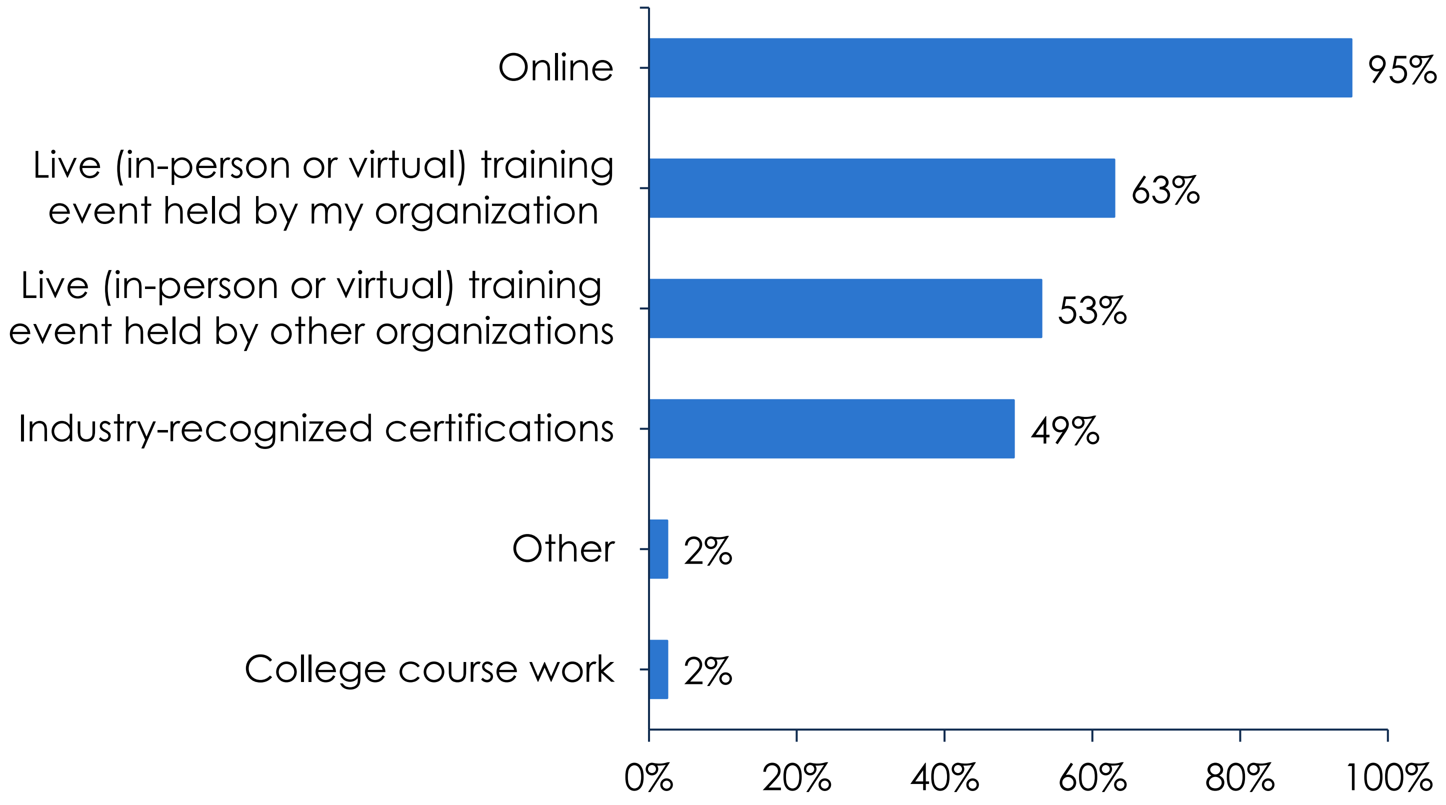
44%: Finding RBT **content** is moderately/very challenging

34%: Finding RBT **guidance** is moderately/very challenging

Strong desire to have **standard training** available to all feds

> "Why does each agency need to develop their own role-based training? Much efficiency could be achieved through centralizing aspects of this." (Q53)

RBT Methods and Formats



How employees can complete RBT (select all that apply)

68% indicated that their organization allows more than one way to complete RBT.

Some organizations allow for employee choice.

> "We allow things like any type of event that's at least one hour in length that is cyber related and also applicable to their specific job duties." (S05)

Tailoring RBT Content

54%: Agreed/strongly agreed that their organization tailors RBT to the **mission**.

58%: Agreed/strongly agreed that their organization tailors RBT to current **security risks**.

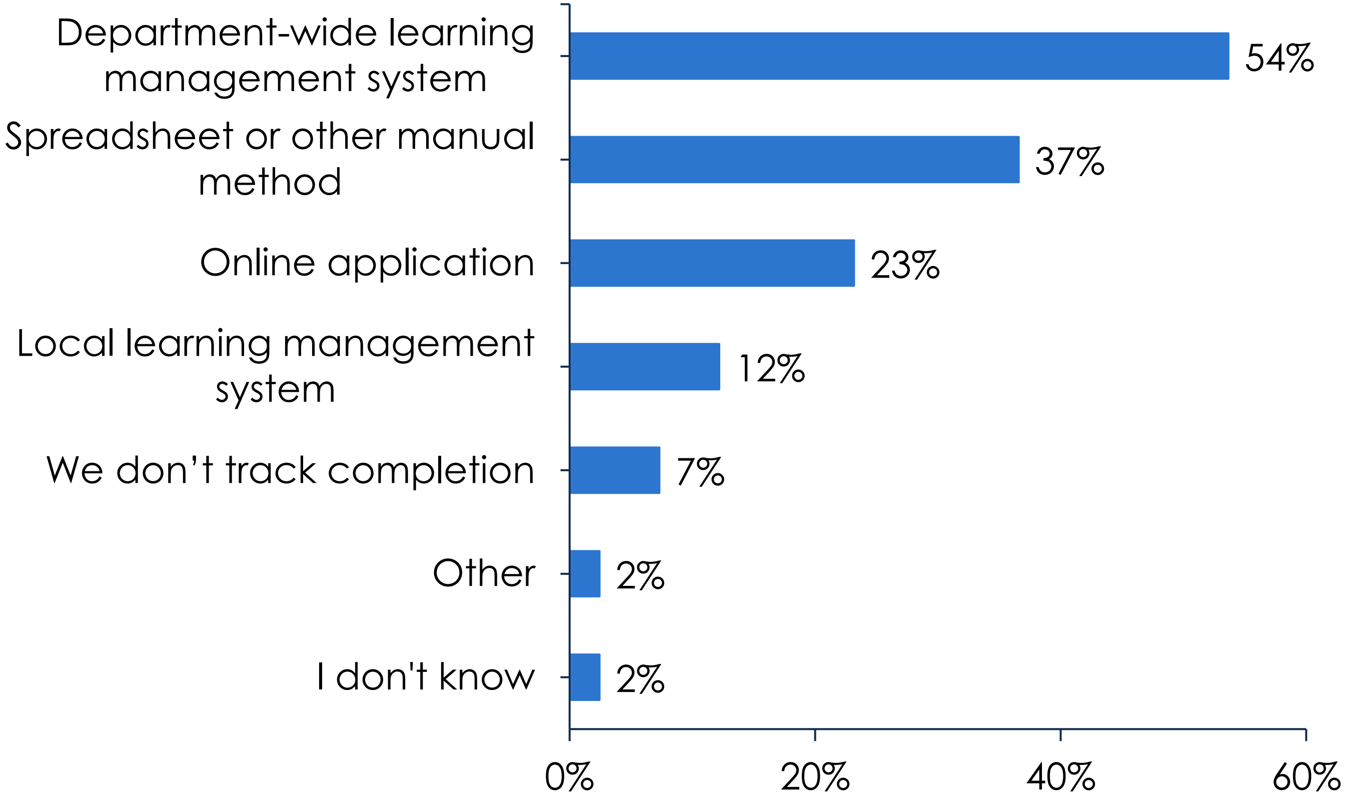
Successes:

"[We bring] ISSOs together to gather the most issues they see so that we could include those issues in the training." (Q30)

Challenges:

"Approach to role-based training is overly tactical, focusing on IT-specific elements (e.g., patching) rather than developing and managing processes that reliably improve cybersecurity outcomes." (Q23)

RBT Completion Tracking



How orgs track RBT completion (select all that apply)

19%: Tracking federal employee RBT completion is moderately/ very challenging

29%: Tracking contractor RBT completion is moderately/very challenging

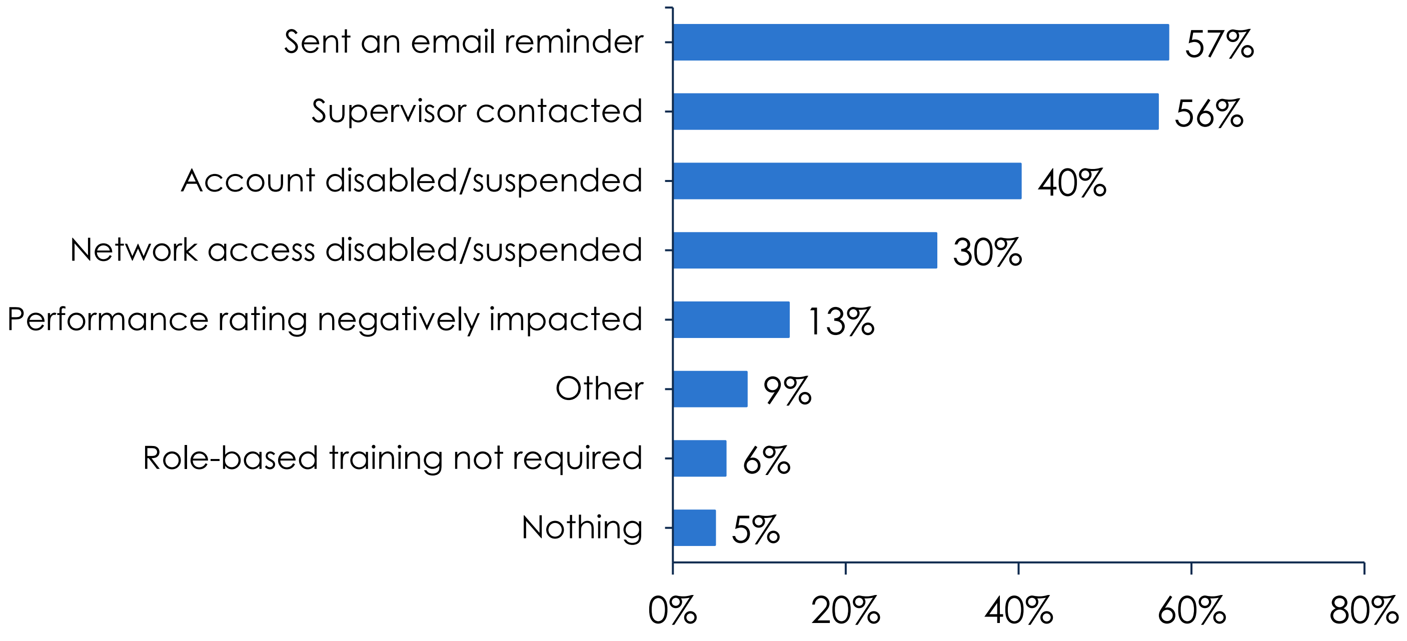
“We've explored self-paced training options, but ensuring compliance and tracking completion is challenging there.” (Q72)

Employees Training Compliance

40%: Getting employees to complete **required** RBT is moderately/very challenging

42%: Getting employees to complete RBT that is **not required** is moderately/very challenging

"There is no time. There are too many duties for the few cyber employees. Training and hands-on always fall to the wayside." (Q59)



What happens if employees fail to complete required RBT (select all that apply)

Workforce Support

65% said *employees* and 70% said *leadership* understand how/why RBT is **relevant** to them.

66% said *employees* and 73% said *leadership* are **supportive** of RBT activities.

Several expressed challenges:

"We do get a lot of pushback where people are saying, 'What does this have to do with my position or what I'm working in at the time?' It's a little frustrating." (N02)

"RBT is not taken seriously by the IT department and leadership at the CIO and above…I have submitted budget requests to improve the program and put comprehensive metrics in place, but they have been denied." (Q29)

RBT Resources

42%: Disagreed/strongly disagreed that they have adequate **funding**

52%: Disagreed/strongly disagreed that they have adequate dedicated **staff**

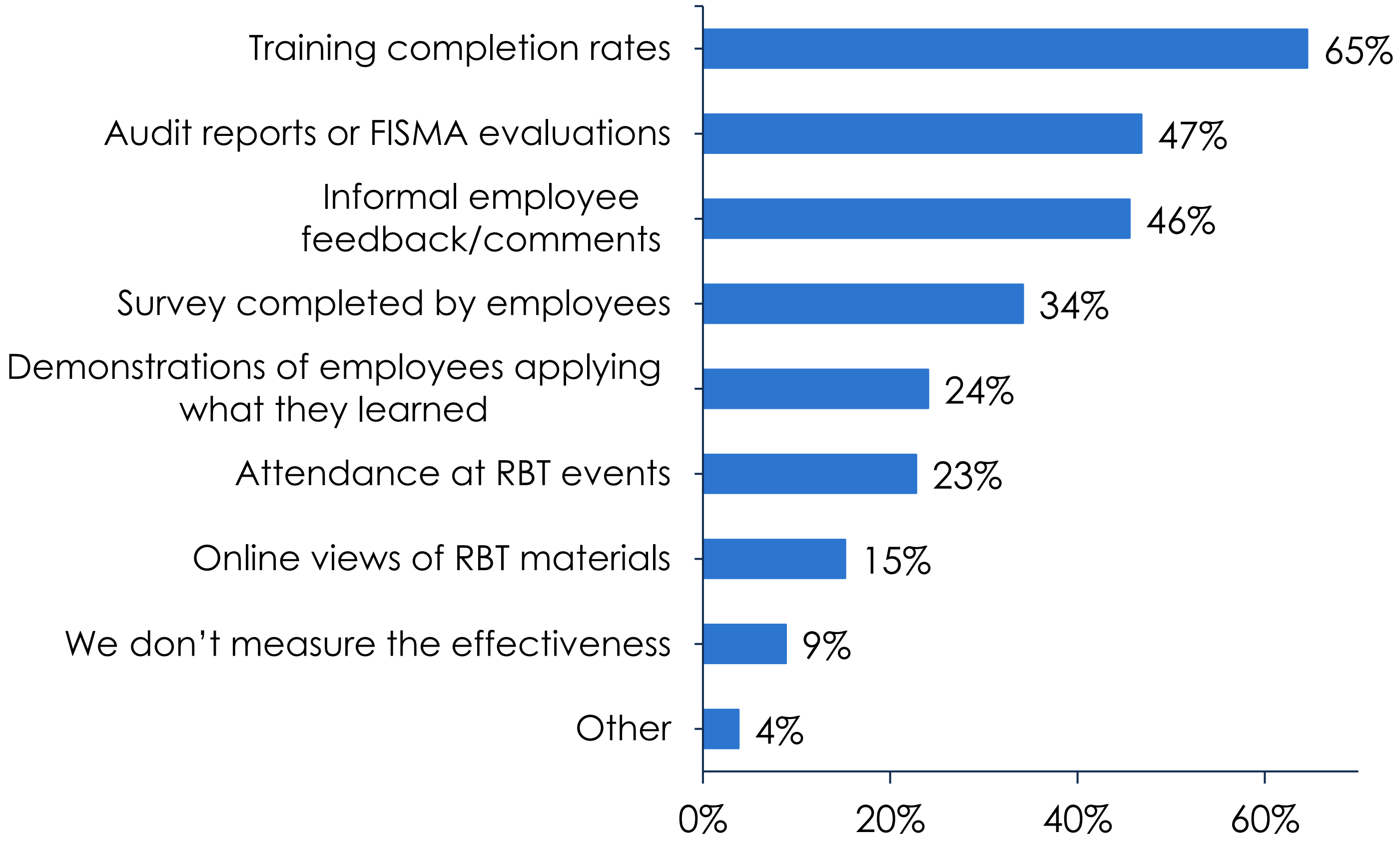
28%: Disagreed/strongly disagreed that they have adequate **technology**

48%: **Getting budgetary support** to improve RBT offerings is moderately/very challenging

"We need to develop training that would help improve the security for every single role and we don't have the resources (time, money) to do it." (Q03)

"Our Agency has 0 dedicated funding and 0 dedicated administrative or human capital resources for role-based training." (Q49)

Measuring Effectiveness of RBT Activities



Measures of RBT effectiveness (select all that apply)

58%: Determining the effectiveness of RBT activities is moderately/very challenging

"More emphasis on measuring the effectiveness of training and some way to prove out/use the skills that were learned from role-based training. People learn best when they have to do a task and if there was modular project that could be used to show the benefits of learning." (Q24)

NIST National Institute of Standards and Technology U.S. Department of Commerce

Perceived Success of RBT Activities

52%: RBT activities are successful/very successful

- 77% in security awareness survey

28%: RBT activities are slightly successful

- 19% in security awareness survey

20%: RBT activities are unsuccessful/very unsuccessful

- 4% in security awareness survey

"[Employees] like the core training we provide and are always asking for follow-up training and refresher courses." (Q75)

"Irrelevant training, and users does not feel motivated in any ways." (Q02)

Advice from the field

The Big Picture

Plan a robust program from the onset

"Get your policies and procedures straight first. Make your processes repeatable and simple." (Q17)

"Create a program plan that describes the mission, vision, and a phased implementation approach, including a continuous learning cycle." (Q52)

Obtain support and prioritize resources

"It's much easier to get management buy-in early in the process and not while you're trying to get your CIO to do the training." (Q03)

"Create the metrics to showcase success." (Q52)

"Prioritize the resources available to meet the critical training gaps." (Q52)

Assign RBT appropriately

"Define based on job roles, not job series." (Q16)

"Clearly communicate WHY an individual is assigned role-based training requirement." (Q33)

Content and Approaches

Seek out existing and updated training

"Identify existing training resources…There are many free and paid training content available online." (Q52)

"Stale training is often worse than no training…Security evolves daily, and the training should reflect this." (Q23)

Tailor RBT to the organization and workforce

"Make the curriculum pertinent to the types of issues your support staff and others have actually had to deal with and solve." (Q70)

"Listen to the business units regarding what they need." (Q75)

Be flexible

"Permit ability to assess-out for those having maturity in role." (Q22)

"Do not require all mandatory courses due at the same time." (Q60)

Thank you!

Jody Jacobs: jody.jacobs@nist.gov
Julie Haney: julie.haney@nist.gov
Susanne Furman: susanne.furman@nist.gov
Group Mailbox: usability@nist.gov

NIST Usable Cybersecurity Program:
https://csrc.nist.gov/usable-cybersecurity

NIST Cybersecurity Awareness Study reports:
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8420.pdf
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8420A.pdf
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8420B.pdf

TRANSFORMING THE FEDERAL CYBER TALENT ECOSYSTEM

Chris Paris

Senior Advisor

Cyber Workforce Management

U.S. Department of Veterans Affairs

Transforming the Federal Cyber Talent Ecosystem

Federal Cyber Workforce Management and Coordinating Working Group

May 2022

The Call for Cyber Talent

Digital Services
UNITED STATES POSTAL SERVICE
NATIONAL WEATHER SERVICE
MedlinePlus
IRS
CDC
NIH

30 days

825 million site visits

40,000 cyber job vacancies

Who We Are

Our Membership

Do Once, Help Many

Pool resources and ingenuity to address shared cyber workforce challenges

Solution-Based Approach

Iteratively develop solutions grounded in the NICE Framework

Our Partners

CHCO COUNCIL

CIO COUNCIL

CLO COUNCIL

What We Found

Entry-Level Cyber Talent

“The incoming and future workforce may use nontraditional routes to enter the cyber workforce (e.g., certifications, boot camps, trade schools).”

Cyber Workforce Development

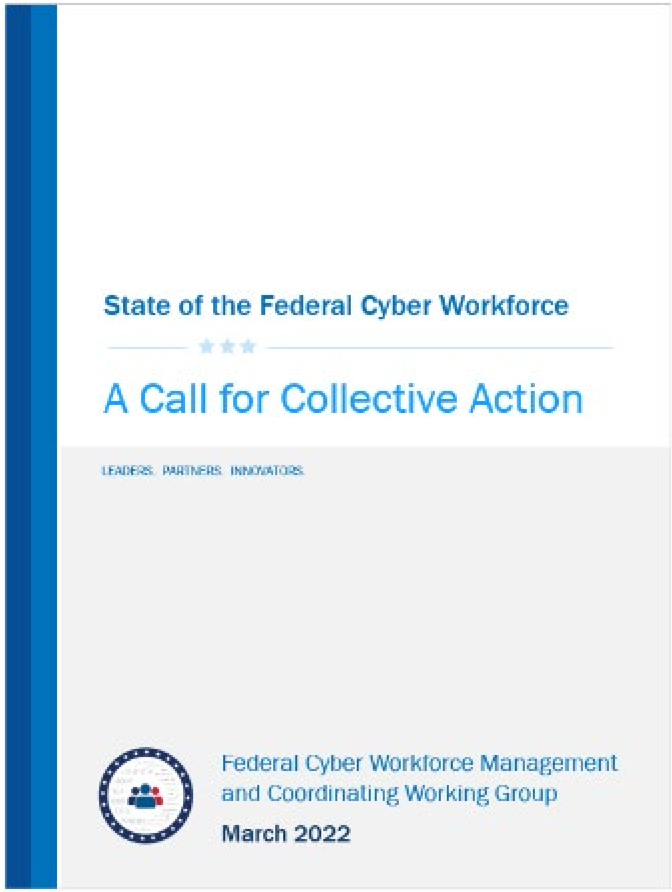
“Employees may not be pursuing training and certifications relevant to their positions.”

“Cyber skills do not transfer well across agencies, minimizing opportunities for movement and growth within the Federal space.”

Cyber Workforce Policy & Classification

Cyber Workforce Data

Cyber Workforce Retention



State of the Federal Cyber Workforce

A Call for Collective Action

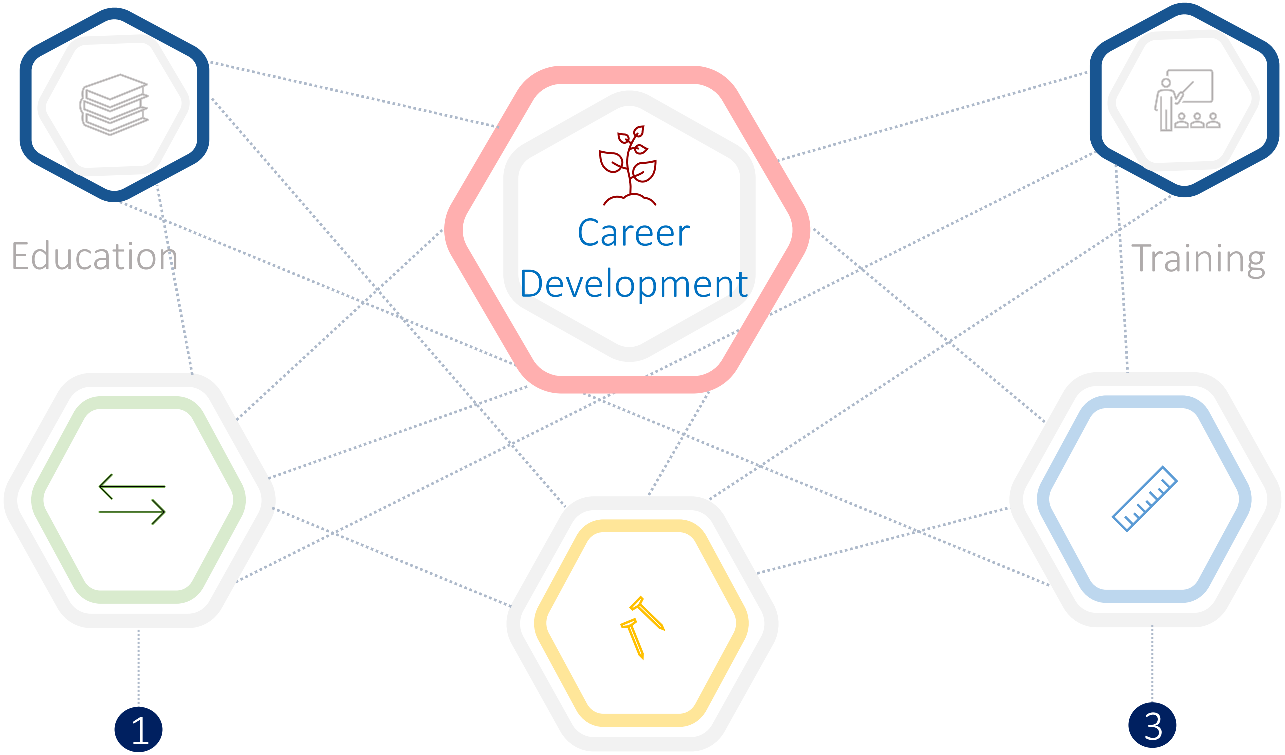
LEADERS. PARTNERS. INNOVATORS.

Federal Cyber Workforce Management and Coordinating Working Group

March 2022

Our Way Forward

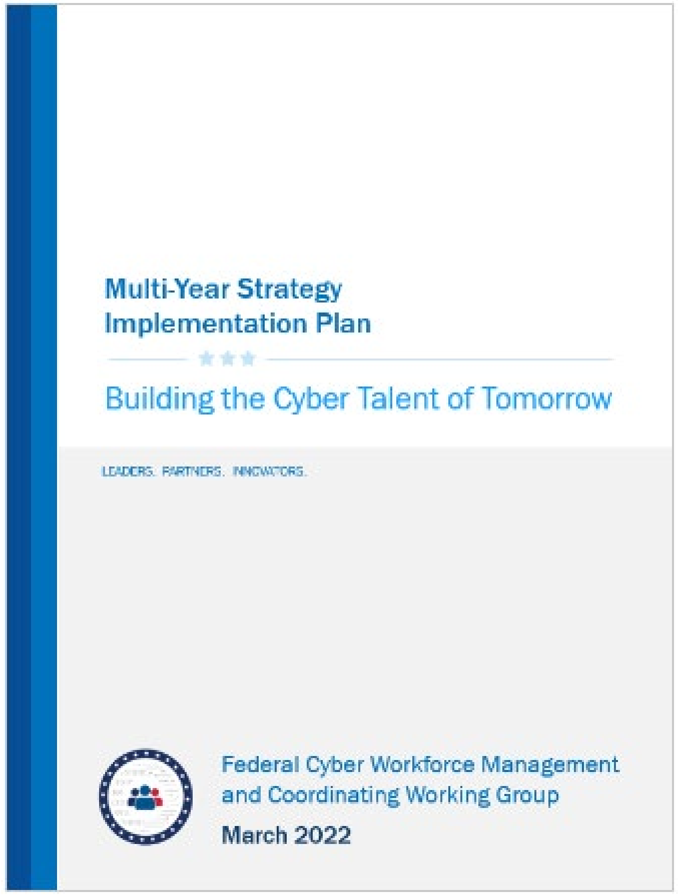
Integrated Ecosystem



1 Streamline skill set development

2 Create career guidance mechanisms

3 Develop skills assessment tools



Multi-Year Strategy Implementation Plan

Building the Cyber Talent of Tomorrow

LEADERS. PARTNERS. INNOVATORS.

Federal Cyber Workforce Management and Coordinating Working Group

March 2022

A Closer Look

Federal Cyber Training Academy

1 Streamline skill set development.

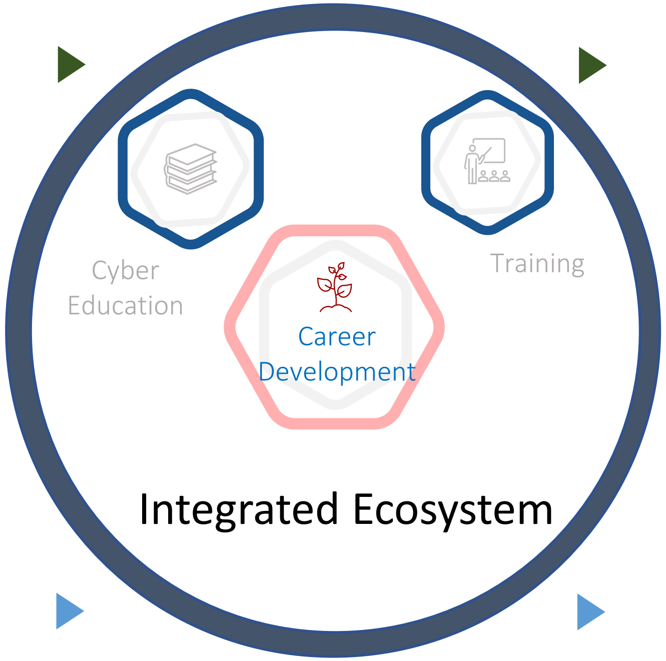
- NICE Framework work role-aligned trainings
- Centralized training catalog
- Cyber Professionals Community

2 Create career guidance mechanisms.

- Career Manager Program Model
- Cyber Career Pathways Tool & Roadmap

3 Develop skills maturity assessments.

- Library of work role-specific assessments
- Collection of work-role specific proficiency indicators



Federal Cyber Professionals

Grow and build skill portfolio.

- Meet minimum qualifications
- Maintain skills
- Diversify capabilities

Progress forward.

- Build personal connections
- Customize a career plan

Gauge skill set growth.

- Identify skill gaps
- Discover areas of strengths

Connect With Us

Chris Paris
Christopher.paris@va.gov

Matt Isnor
Matthew.m.isnor.civ@mail.mil

Megan Caposell
Megan.caposell@cisa.dhs.gov

For more information on the Working Group, visit our page on the OMB Max Portal:

https://community.max.gov/x/uJ37YQ

CLOSING REMARKS

Maureen Premo

FISSEA Co-Chair

Immigration and Customs Enforcement

Department of Homeland Security

THANK YOU

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

https://www.surveymonkey.com/r/2022fisseaspringforum

fissea FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

LOOKING FORWARD

GET INVOLVED

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

Volunteer for the Planning Committee
Email FISSEA@nist.gov

Serve on the Contest or Award Committees for 2022

FISSEA FALL FORUM

Theme: Role Based Training

November 15, 2022
1:00pm – 4:00pm ET

REGISTER TODAY:
nist.gov/fissea

LOOKING FORWARD

THANK YOU

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

https://www.surveymonkey.com/r/2022fisseaspringforum

fissea FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

#FISSEA2022 | NIST.GOV/FISSEA

LOOKING FORWARD