NIST Cybersecurity Framework (CSF) 2.0: Overview & Resources

Cherilyn Pascoe
Director, NIST National Cybersecurity Center of Excellence (NCCoE)
October 2024

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

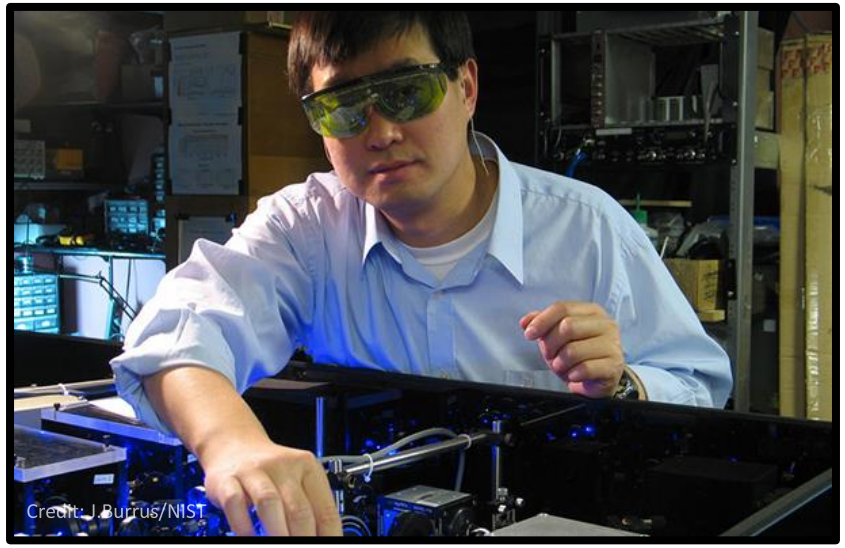
Agenda

- Introduction
- Brief Overview of NIST CSF
- What Has Changed with CSF 2.0
- Suite of CSF 2.0 Resources – including those for healthcare
- Q&A

NIST's Mission

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

To promote U.S. innovation and industrial competitiveness by advancing **measurement science, standards, and technology** in ways that enhance economic security and improve our quality of life



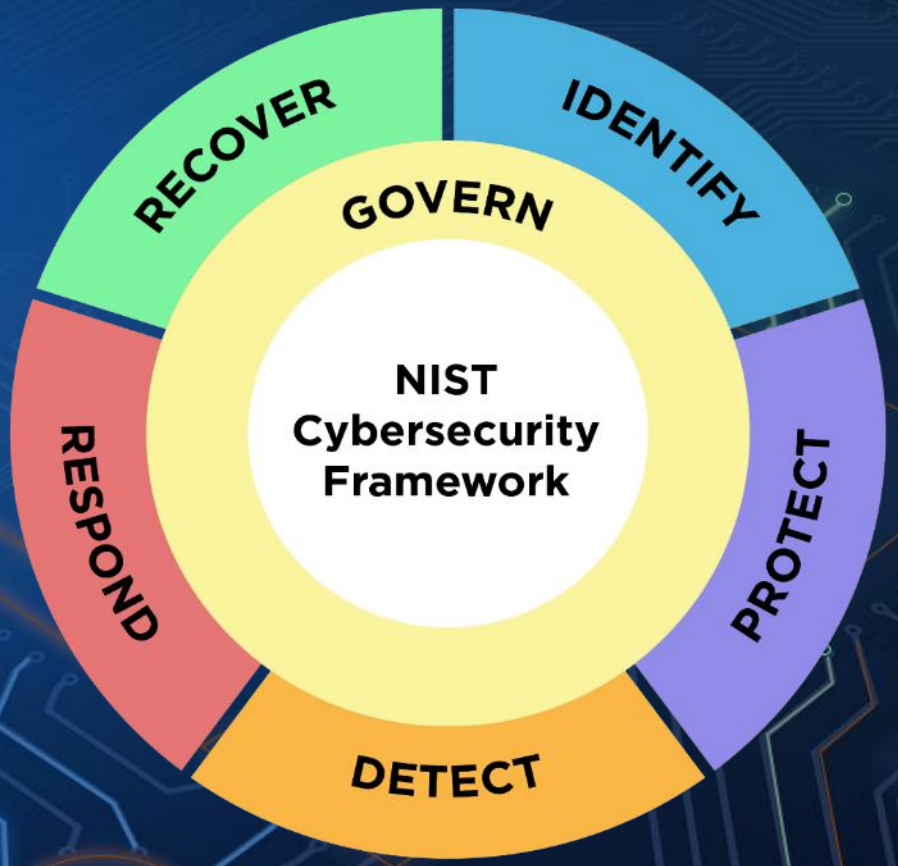
NIST's Priority Areas in Cybersecurity and Privacy

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

Enhancing risk management	Privacy	Strengthening cryptographic standards and validation
Cybersecurity awareness, training, and education and workforce development	Metrics and measurements	Identity and access management
Trustworthy networks	Trustworthy platforms	Securing emerging technologies

Source: "*2021: What's Ahead from NIST in Cybersecurity and Privacy?*" By Kevin Stine, https://www.nist.gov/blogs/cybersecurity-insights/2021-whats-ahead-nist-cybersecurity-and-privacy

Brief Overview of CSF 2.0



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

https://www.nist.gov/cyberframework

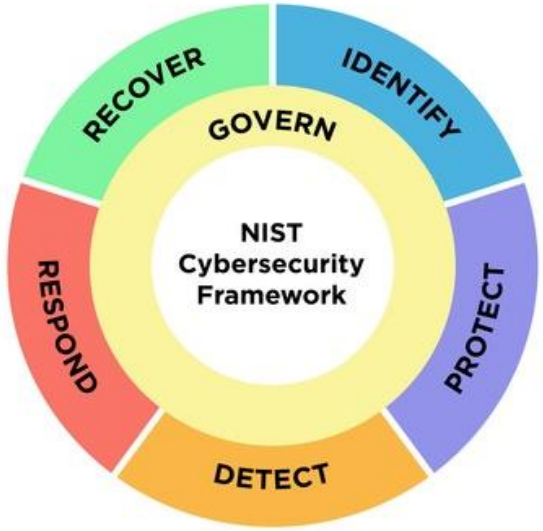
NIST Cybersecurity Framework

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

The NIST Cybersecurity Framework (CSF) helps organizations reduce their cybersecurity risks and is widely recognized as foundational to securing organizations & technology.

What is it?

- Comprehensive list of cybersecurity outcomes to reduce cybersecurity risks to an organization – the “what”, not “how” or “who”
- Based on and mapped to international standards and resources
- Adaptable to many technologies, sectors, maturity levels, and uses



How is it used?

- **Understand and Assess:** Describe the current or target cybersecurity posture of part or all of an organization, determine gaps, and assess progress toward addressing those gaps.
- **Prioritize:** Identify, organize, and prioritize actions for managing cybersecurity risks that align with the organization’s mission, legal and regulatory requirements, and risk management and governance expectations.
- **Communicate:** Provide a common language for communicating inside and outside the organization about cybersecurity risks, capabilities, needs, and expectations.

NIST Cybersecurity Framework 2.0

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

Voluntary guidance that helps organizations—regardless of size, sector, or maturity— better **understand, assess, prioritize**, and **communicate** their cybersecurity efforts.

**not a one-size-fits-all approach to managing cybersecurity risks.*

CSF Core	CSF Organizational Profiles	CSF Tiers
The nucleus of the CSF. **A taxonomy of high-level cybersecurity outcomes** that can help any organization manage its cybersecurity risks. Functions>Categories>Subcategories	A mechanism for describing an organization's **current and/or target cybersecurity posture** in terms of the CSF Core's outcomes.	Characterize the **rigor** of an organization's cybersecurity risk governance and management practices. Tiers can also provide **context** for how an organization views cybersecurity risks and the processes in place to manage those risks.

https://www.nist.gov/cyberframework

Global Impact of CSF 2.0

- The CSF is used widely **internationally**.
- NIST's work with the **International Organization for Standardization (ISO)**, in conjunction with the **International Electrotechnical Commission (IEC)**, over the last 11 years has been expansive.
- The resources allow organizations to build cybersecurity frameworks and organize controls using the CSF Functions.

Translations:

- CSF 1.1 and 1.0 – **13 languages**
- CSF 2.0 – **Portuguese** and **Spanish**
- The Small Business (SMB) Quick-Start Guide – **Portuguese**, **Spanish**, and **French**

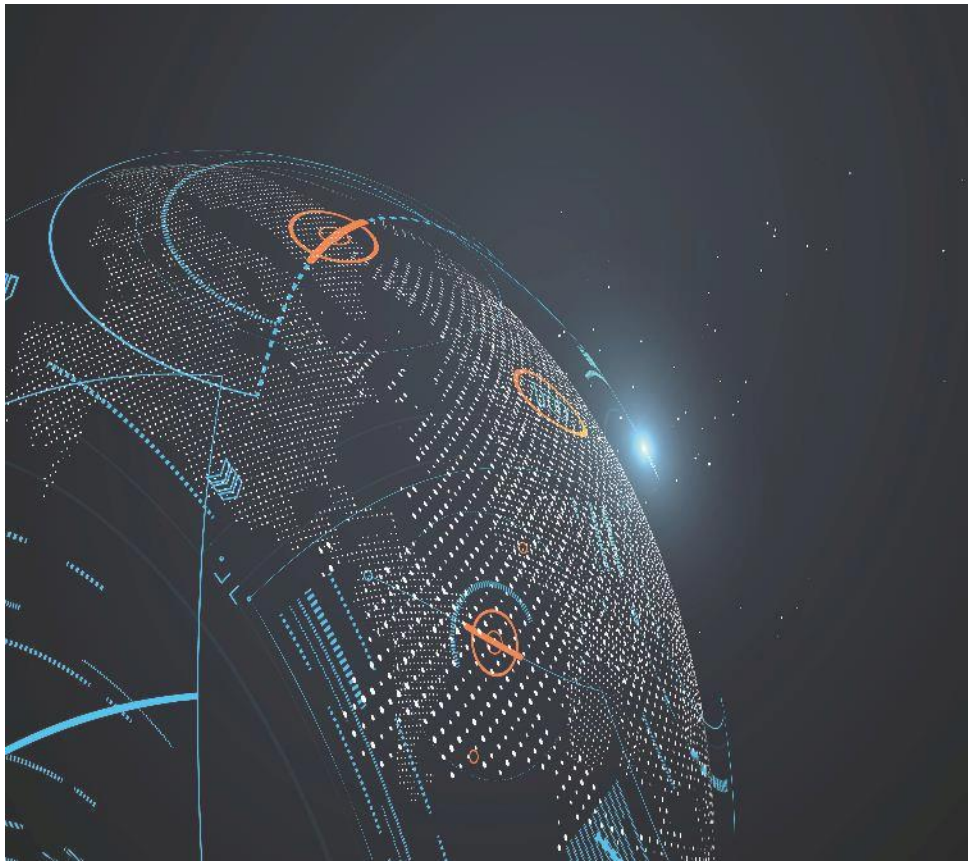
Learn more about our global impact: www.nist.gov/cyberframework

Governmental Policies on CSF

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

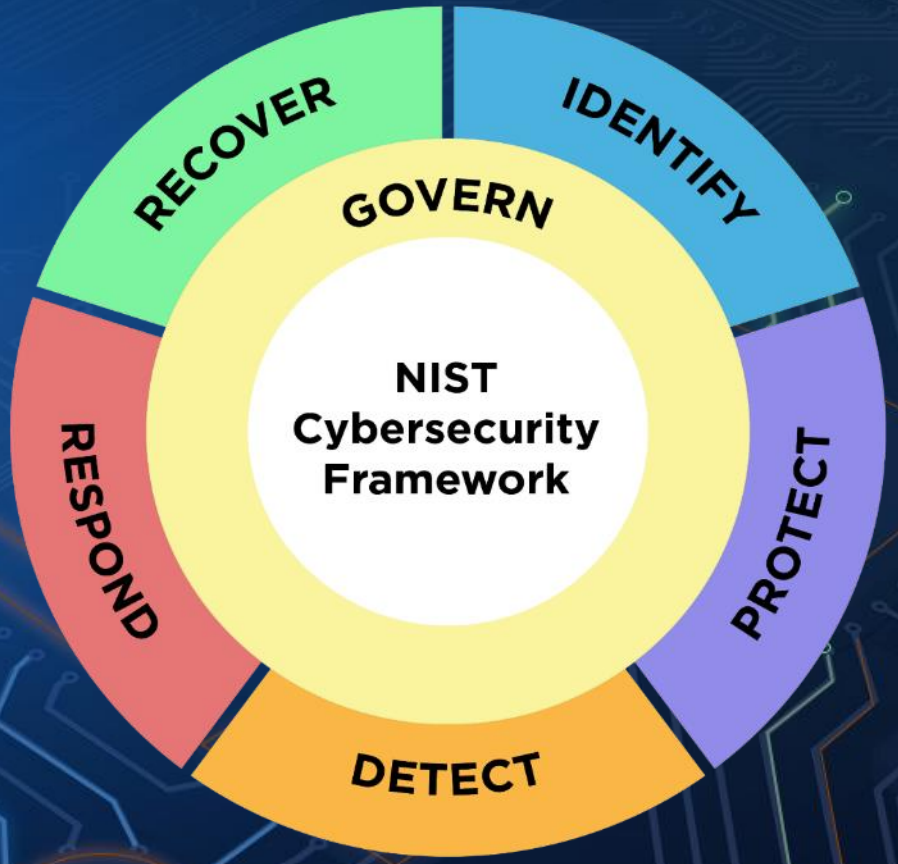
Adapted in several countries and regions

- United States (federal and state)
  - **The White House National Cybersecurity Strategy (March 2023): https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf**
    - "Regulations should be performance-based, leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance – including the Cybersecurity and Infrastructure Security Agency (CISA)'s Cybersecurity Performance Goals and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity – …"
- Italy, Poland, Israel, Japan, Uruguay, Australia, and more



Examples highlighted on the NIST International Cybersecurity and Privacy Resource Site:
https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources

CSF 2.0



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

https://www.nist.gov/cyberframework

How Did We Get Here?

The CSF has been developed through an iterative, community-driven process since 2013.

CSF 2.0 | What is Driving Change?

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

Stakeholder Insights – What *You* Needed!

Shifting Threat & Technology Environment

Evolving Enterprise Risk Management

The Existing Roadmap & Sector Profile Inputs

Changes in CSF 2.0 for Healthcare

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

Applies to ***all organizations*** – not just those in critical infrastructure.	Regardless of a healthcare organization's size or resources, there is a framework in place to safeguard health data against cyber threats.
Incorporates an entirely new function to address ***"Governing" risk management*** processes.	Provides an opportunity to align organizational goals and compliance requirements (HIPAA).
Integrates Supply Chain throughout!	Focuses on third-party vendors and partners.
Focuses on ***continual improvement***.	Recognizes that cybersecurity is an evolving field and should adapt to new threats and technologies.
Provides a ***suite of resources*** (not one document).	Offers more guidance to help small businesses and specific use cases.
Encourages ***global*** use and collaboration.	Provides a collaborative approach to cybersecurity risk management.

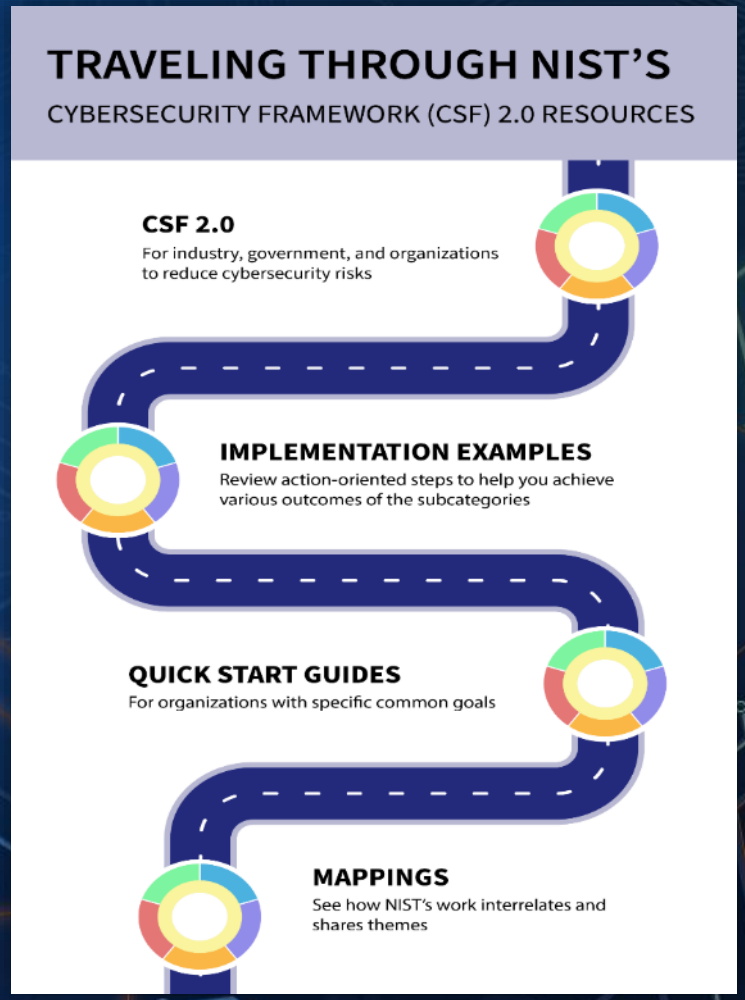
CSF 2.0 Core

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

Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

NIST CSF 2.0 Resources

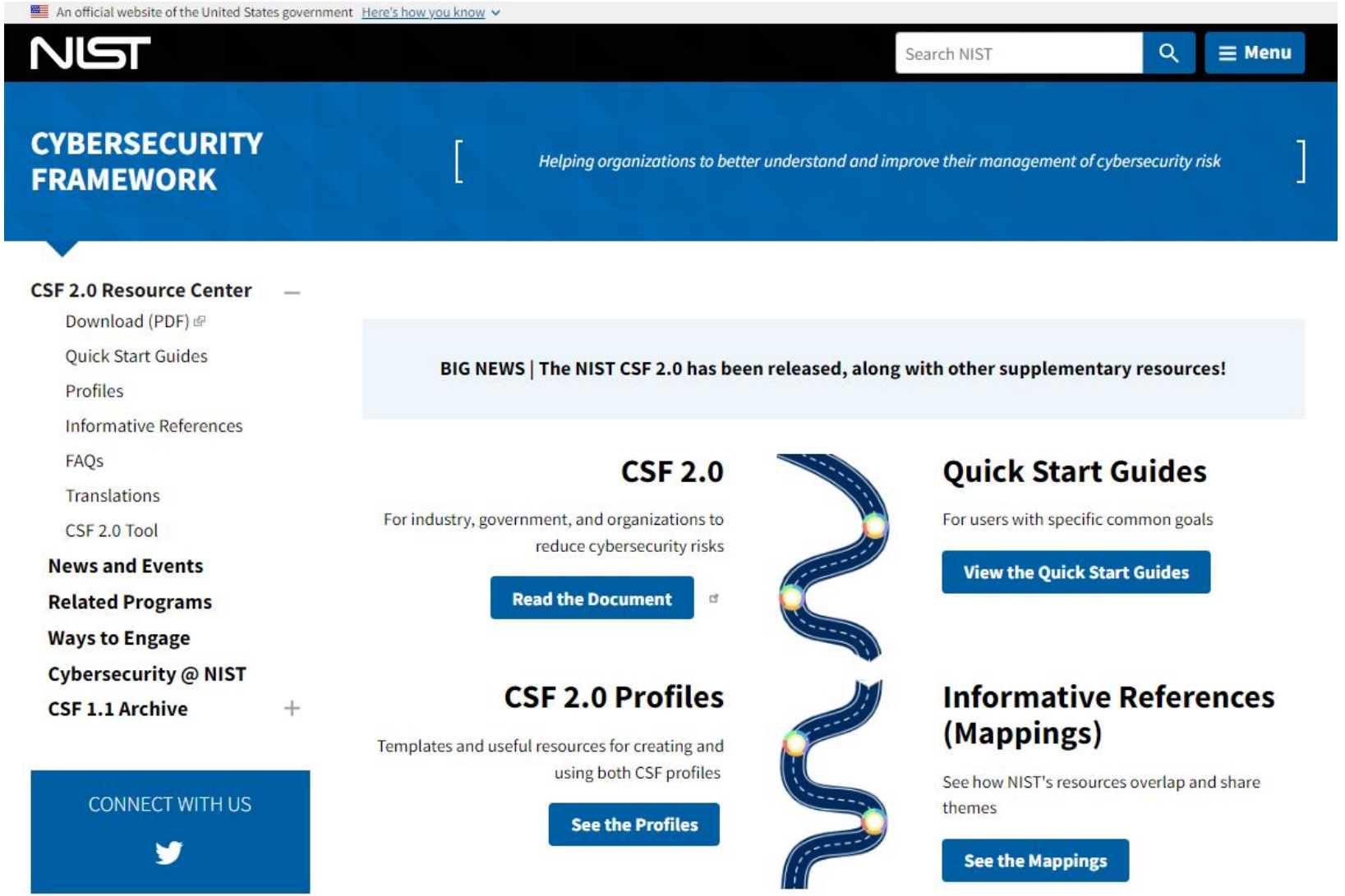


NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

https://www.nist.gov/cyberframework

CSF 2.0 Resource Library

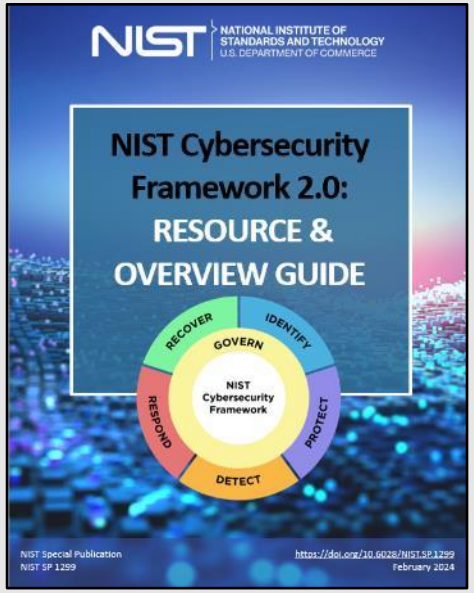
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



https://www.nist.gov/cyberframework

Suite of CSF 2.0 Resources

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



Navigating NIST's CSF 2.0 Quick Start Guides

Resource and Overview Guide

Understand the basics and learn about the many available helpful CSF 2.0 resources

Download

The below targeted guides will help you with specific topics.

CSF 2.0 Organizational Profiles
Guidance for organizations, with considerations for creating and using spreadsheets called *Profiles*, to implement the CSF 2.0.

Download

CSF 2.0 Community Profiles
This guide provides considerations for creating and using Community Profiles to implement the CSF 2.0 and support the needs of organizations in communities that share common priorities.

Download

Small Business
Resources specifically tailored to small businesses with modest or no cybersecurity plans currently in place.

Download

C-SCRM
Helps organizations become smarter acquirers and suppliers of technology products and services.

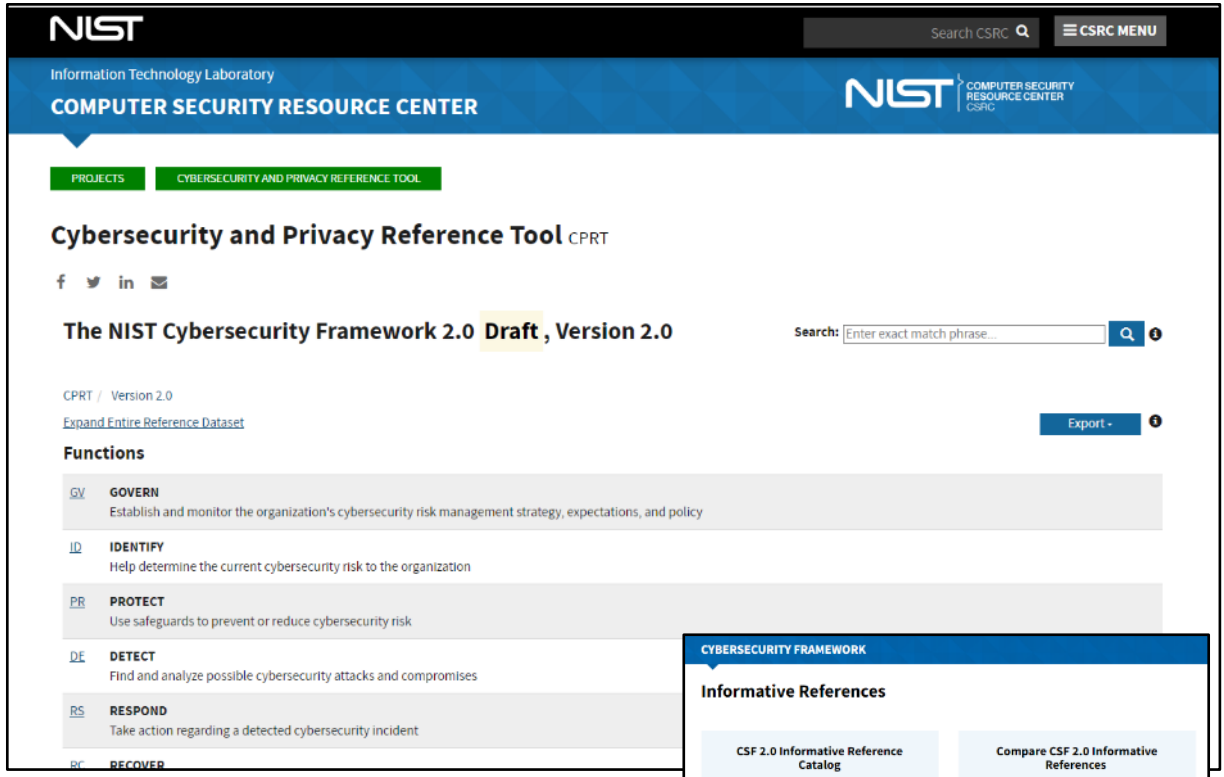
Download

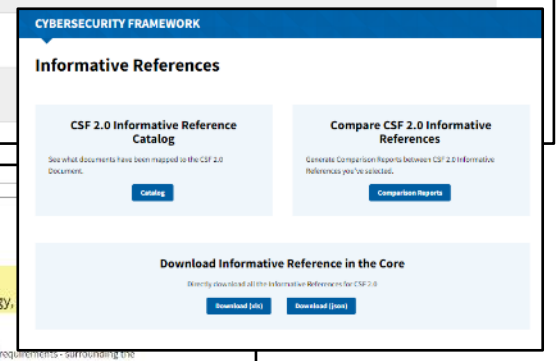
Tiers
Organizations can use these to apply the CSF 2.0 Tiers to Profiles to characterize the rigor of their cybersecurity risk governance and management outcomes.

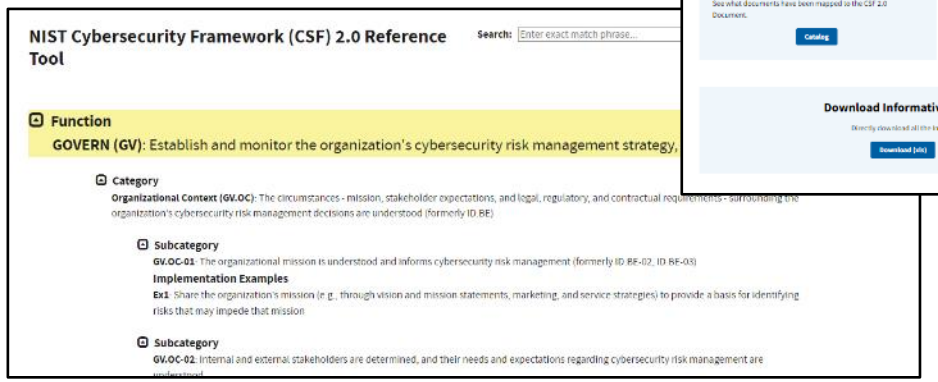
Download

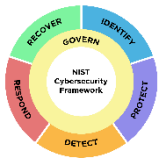
Enterprise Risk Management
How ERM practitioners can utilize the outcomes provided in the CSF 2.0 to improve organizational cybersecurity risk management.

Download









CSF Resources for Healthcare

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

CPRT Mapping of HIPAA to CSF 1.1

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

Category	Subcategory	Reference Items
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. Hide all ID.AM References + ID.AM to Cybersecurity Framework v2.0 + ID.AM to SP 800-221A + NIST SP 800-37 Revision 2 to ID.AM + NISTIR-8286 to ID.AM + NISTIR-8286A to ID.AM + SCFv2023.2 to ID.AM + SP 800-221A to ID.AM	**ID.AM-1:** Physical devices and systems within the organization are inventoried Hide all ID.AM-1 References + CIS Controls to ID.AM-1 + COBIT 2019 to ID.AM-1 + Department of Energy - C2M2 to ID.AM-1 – HIPAA Security Rule to ID.AM-1 • ID.AM-1 ↔ 164.308(a)(1)(ii)(A) • ID.AM-1 ↔ 164.310(a)(2)(ii) • ID.AM-1 ↔ 164.310(d) • ID.AM-1 ↔ 164.310(d)(2)(i) • ID.AM-1 ↔ 164.310(d)(2)(ii) • ID.AM-1 ↔ 164.310(d)(2)(iii) • ID.AM-1 ↔ 164.310(d)(2)(iv) + HITRUST CSF v9.2 to ID.AM-1 + HITRUST CSF v9.3.1 to ID.AM-1 + HITRUST CSF v9.6x to ID.AM-1	**CIS CSC**: 1 **COBIT 5**: BAI09.01, BAI09.02 **ISA 62443-2-1:2009**: 4.2.3.4 **ISA 62443-3-3:2013**: SR 7.8 **ISO/IEC 27001:2013**: A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4**: CM-8, PM-5

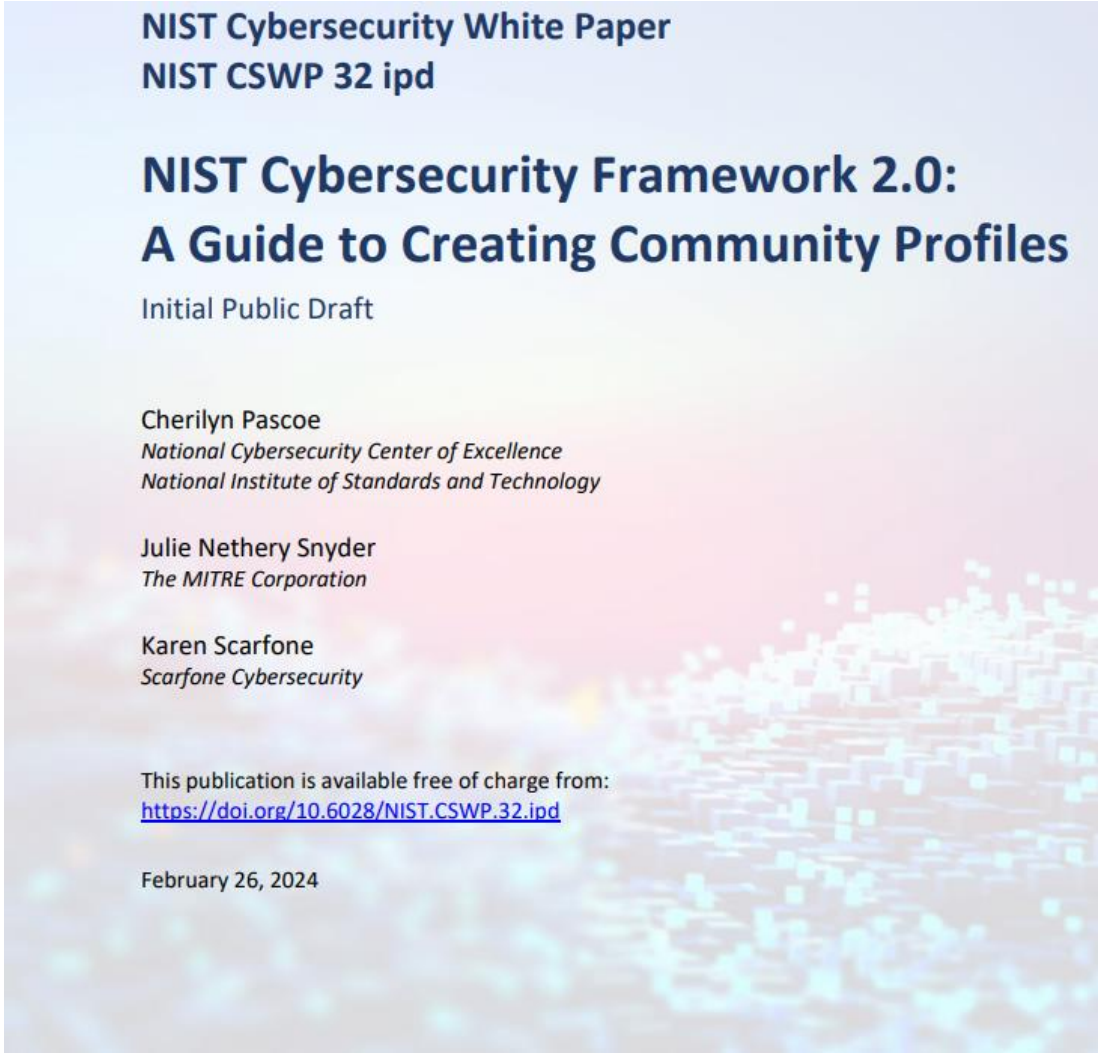
More details: Cybersecurity and Privacy Reference Tool | CSRC (nist.gov)

CSF 2.0 Community Profiles

- Guidance for a specific context (sector, technology, or challenge) that is organized around the common taxonomy of the CSF.
- Defines interests, goals, and outcomes to find consensus on priorities for that community

CSF 2.0 Outcome		Priority	Rationale	Informative References / Mappings
ID.AM-01	Inventories of hardware managed by the organization are maintained			
ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained			

Table 1 Sample Community Profile Template



CSF 2.0 Community Profiles

- **CSF 1.1 – HPH Sector Coordinating Council Health Care and Public Health Sector Cybersecurity Framework Implementation Guide (2023)**
- NIST SP 800-61 Rev. 3 ipd, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile
- CRI Profile for the Financial Sector - Cyber Risk Institute

In Development:

- AI Cybersecurity
- Ransomware
- Semiconductor Manufacturing
- Genomic Data (CSF/Privacy Framework)

NIST NCCoE Framework Resource Center: https://www.nccoe.nist.gov/framework-resource-center

NCCoE Healthcare Work Leveraging CSF – Mappings of Technology Products to the CSF

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

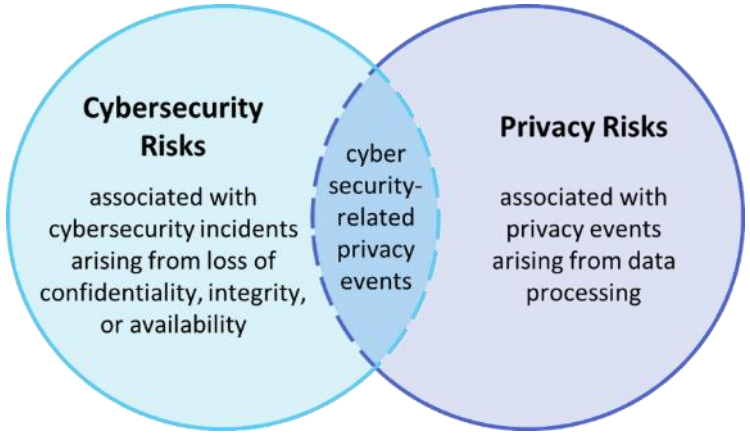
NIST SP 1800-1: Securing Electronic Health Records on Mobile Devices

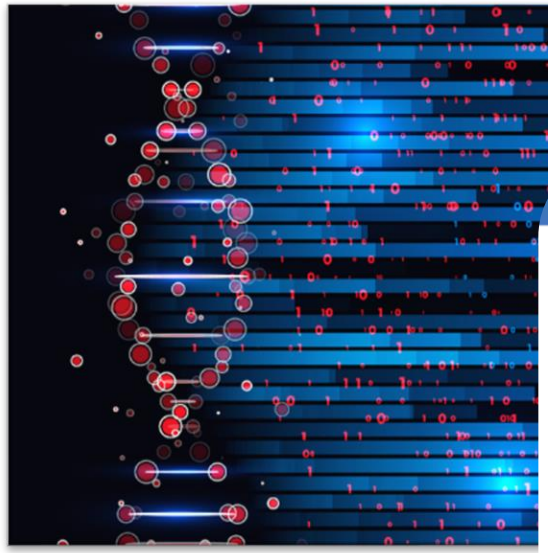
NIST SP 1800-8: Securing Wireless Infusion Pumps (WIP) in Healthcare Delivery Organizations

NIST SP 1800-24: Securing Picture Archiving and Communications Systems

NIST SP 1800-30: Securing Telehealth Remote Patient Monitoring Ecosystem

Upcoming:
NIST IR 8467: Integrated Cybersecurity and Privacy Framework Profile for Genomic Data





STATUS: PREPARING DRAFT

The public comment period has closed for NIST IR 8467, *Cybersecurity Framework Profile for Genomic Data*.

We are currently updating the document based on the recently released Cybersecurity Framework 2.0 and developing a Privacy Framework 1.0 Profile. The next release will be an integrated Cybersecurity and Privacy Framework Profile for Genomic Data.

NIST IR 8467 Cybersecurity Framework Profile for Genomic Data (Initial Public Draft)

NIST IR 8432 Cybersecurity of Genomic Data

Key Takeaways

- NIST standards and guidance help safeguard the nation's critical infrastructure, including healthcare.
- Anyone can download our freely available cybersecurity guidance and resources.
- Organizations can use our reference architectures to implement secure technology solutions.
- We are forward-looking – we incorporate technology concepts influencing the healthcare sector into our cybersecurity guidance.
- None of our cybersecurity guidance would be applicable without the expertise of our project collaborators.
- Cybersecurity risk management is always a journey – and the CSF 2.0 is a navigational guide that can help make that journey more successful.

Share with us your experiences with the CSF – we continue to encourage candid, constructive discussions around the CSF.

List of Resources

Quick Links	Contact Information
CSF 2.0 Website: https://www.nist.gov/cyberframework **CSF 2.0 FAQs:** https://www.nist.gov/faqs	cyberframework@nist.gov
NCCoE Community Profiles: https://www.nccoe.nist.gov/framework-resource-center https://www.nccoe.nist.gov/projects/guide-creating-community-profiles	framework-profiles@nist.gov
CSF 2.0 Small Business Quick Start Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf	smallbizsecurity@nist.gov
Cybersecurity and Privacy Reference Tool (CPRT): https://csrc.nist.gov/Projects/cprt -	cprt@nist.gov
NCCoE Healthcare Portfolio: https://www.nccoe.nist.gov/healthcare https://www.nccoe.nist.gov/projects/cybersecurity-and-privacy-genomic-data	hit_nccoe@nist.gov genomic_cybersecurity_nccoe@nist.gov

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

STAY IN TOUCH

CONTACT US

nist.gov
nccoe.nist.gov

@NISTcyber

Email us: cyberframework@nist.gov or nccoe@nist.gov

Introduction to the National Cybersecurity Center of Excellence (NCCoE)

Cherilyn Pascoe, Director
National Institute of Standards and Technology (NIST),
National Cybersecurity Center of Excellence (NCCoE)

Thursday, October 24, 2024

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

Who We Are

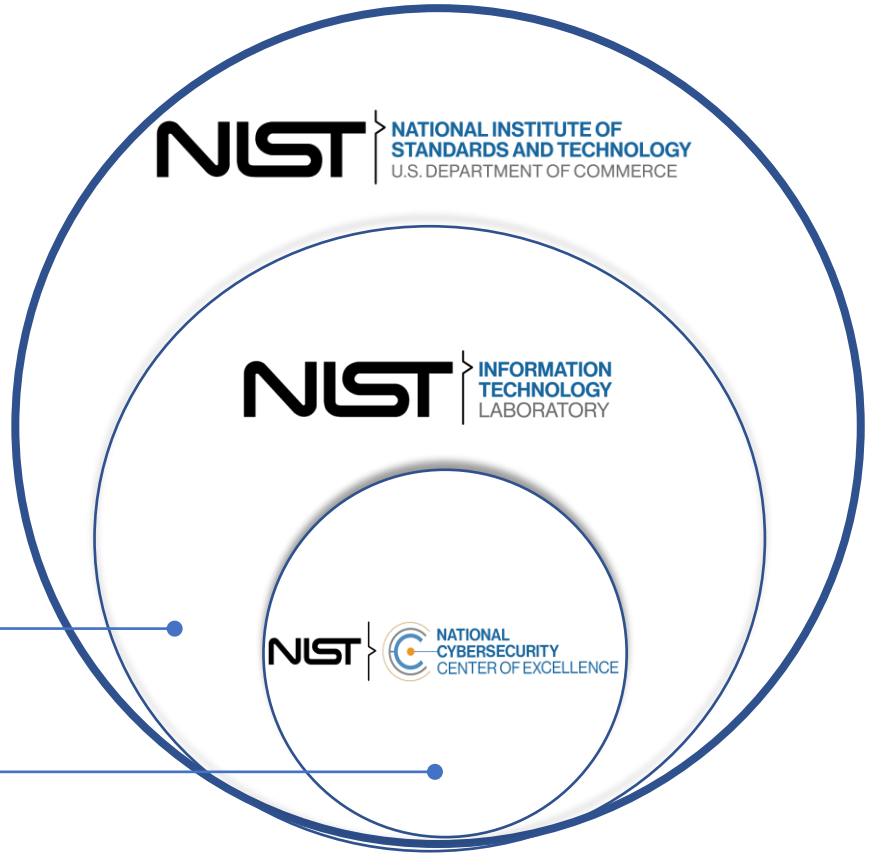
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

A **solution-driven**, **collaborative** hub addressing complex cybersecurity problems

Who We Are

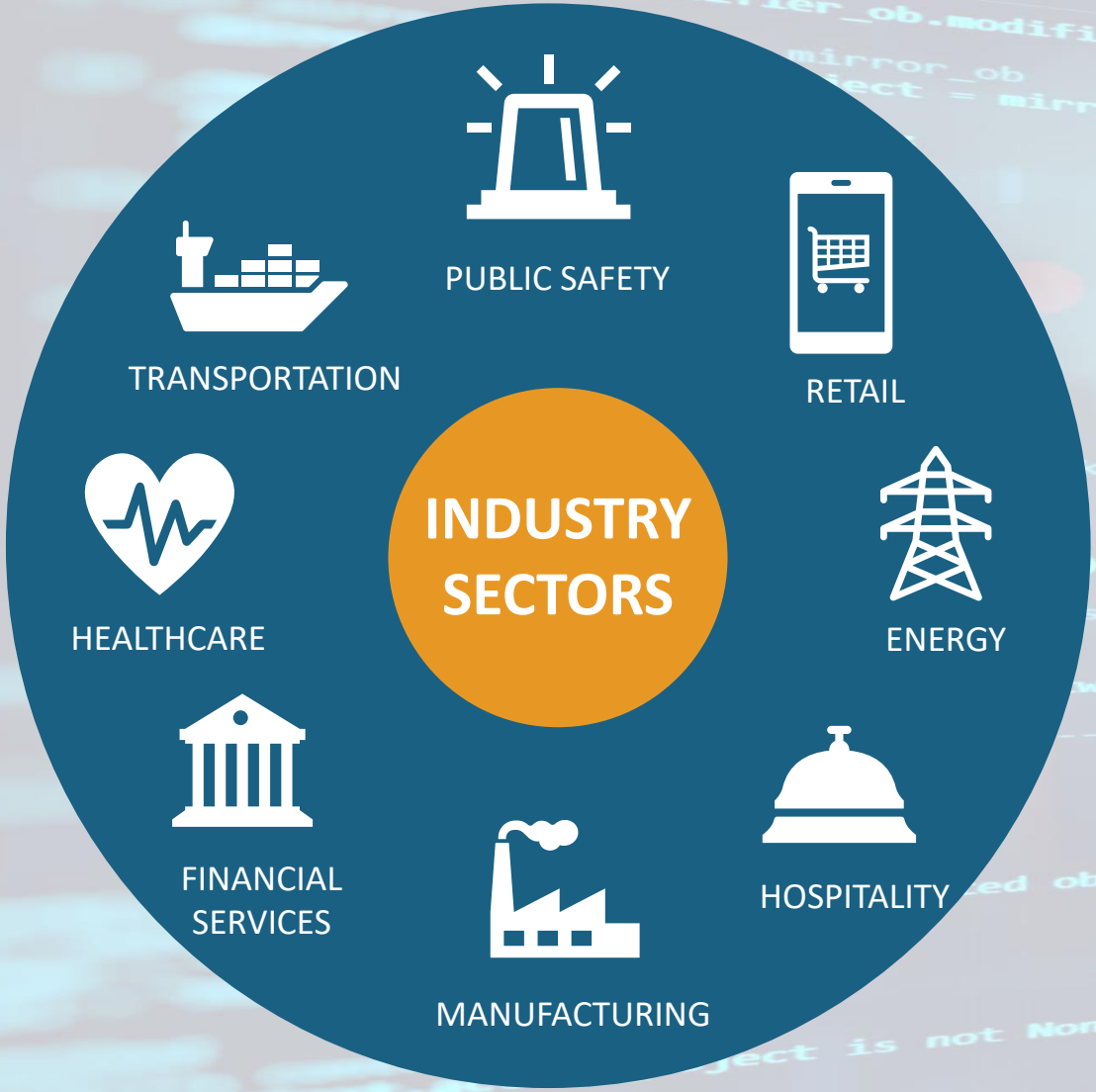
As part of the NIST family, the NCCoE has access to a foundation of expertise, resources, relationships, and experience.

NIST is a **non-regulatory** agency. Our guidance is **voluntary**.



Guidance Created With Industry, For Industry

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



SECURITY GUIDANCE | OUR APPROACH | NEWS & INSIGHTS | GET INVOLVED | SEARCH

By Technology

- 5G Cybersecurity
- Applied Cryptography
- Artificial Intelligence
- Critical Cybersecurity Hygiene
- Cybersecurity for the Space Domain
- Data Classification
- Data Security
- DevSecOps
- Digital Identities - mDL
- Genomics Cybersecurity
- Internet of Things (IoT)
- IPv6
- Mobile Device Security
- Supply Chain Assurance
- Trusted Cloud
- Zero Trust Architecture

By Sector

- Consumer Data Protection
- Energy
- Financial Services
- Healthcare
- Manufacturing
- Public Safety/First Responder
- Water/Wastewater

By Community

- Framework Resource Center

By Status

- Defining Scope
- Seeking Collaborators
- Preparing Draft
- Soliciting Comments
- Reviewing Comments
- Finalized Guidance
- Archived

NCCoE Healthcare Portfolio

NIST SP 1800-1: Securing Electronic Health Records on Mobile Devices

NIST SP 1800-8: Securing Wireless Infusion Pumps (WIP) in Healthcare Delivery Organizations

WIP DEMO VIDEO: https://youtu.be/5XMILRdx_AE

NIST SP 1800-24: Securing Picture Archiving and Communications Systems

Interactive Practice Guide: https://www.nccoe.nist.gov/publication/1800-24-ipg/

NIST SP 1800-30: Securing Telehealth Remote Patient Monitoring Ecosystem

Current Projects:

- Mitigating Cybersecurity Risk in Telehealth Smart Home Integration (SHI)
- Cybersecurity of Genomic Data

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

HIPAA Security Rule Conference Fall 2024

NIST National Cybersecurity Center of Excellence (NCCoE) Healthcare Cybersecurity Projects Panel

Panelists

- **Seth Carmody**, VP, Regulatory Strategy - Medcrypt
- **Roberto Suarez**, VP, Chief Information Security Officer - Carefirst Bluecross Blueshield
- **Sue Wang**, Principal Cybersecurity Engineer - MITRE
- **Cherilyn Pascoe**, Director (Moderator), - National Cybersecurity Center of Excellence (NCCoE), National Institute of Standards and Technology (NIST)

Related Resources

Medcrypt

- https://www.medcrypt.com

Carefirst Bluecross Blueshield

- https://carefirst.com

MITRE

- https://www.mitre.org

NIST

- NCCoE Healthcare Sector: https://www.nccoe.nist.gov/healthcare

Safeguarding Health Information: The Role of the Cybersecurity Workforce

Karen A. Wetzel, Lead, NICE Framework
karen.wetzel@nist.gov
National Institute of Standards and Technology (NIST)
U.S. Department of Commerce

Safeguarding Health Information: Building Assurance through HIPAA Security | October 24, 2024

NIST | NICE

NICE Mission

To energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development.

www.nist.gov/nice

NIST | NICE

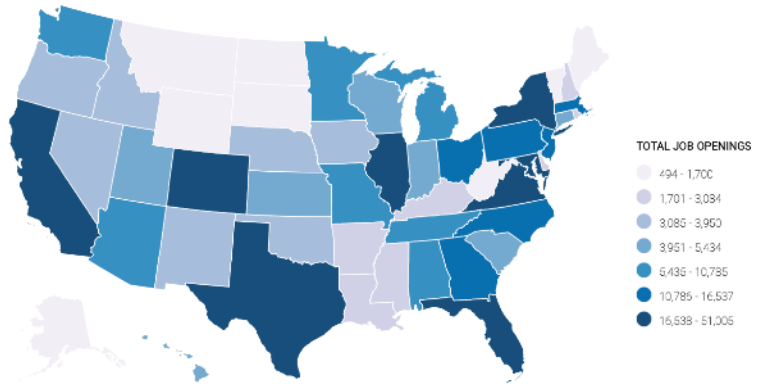
What is the Cybersecurity Workforce?

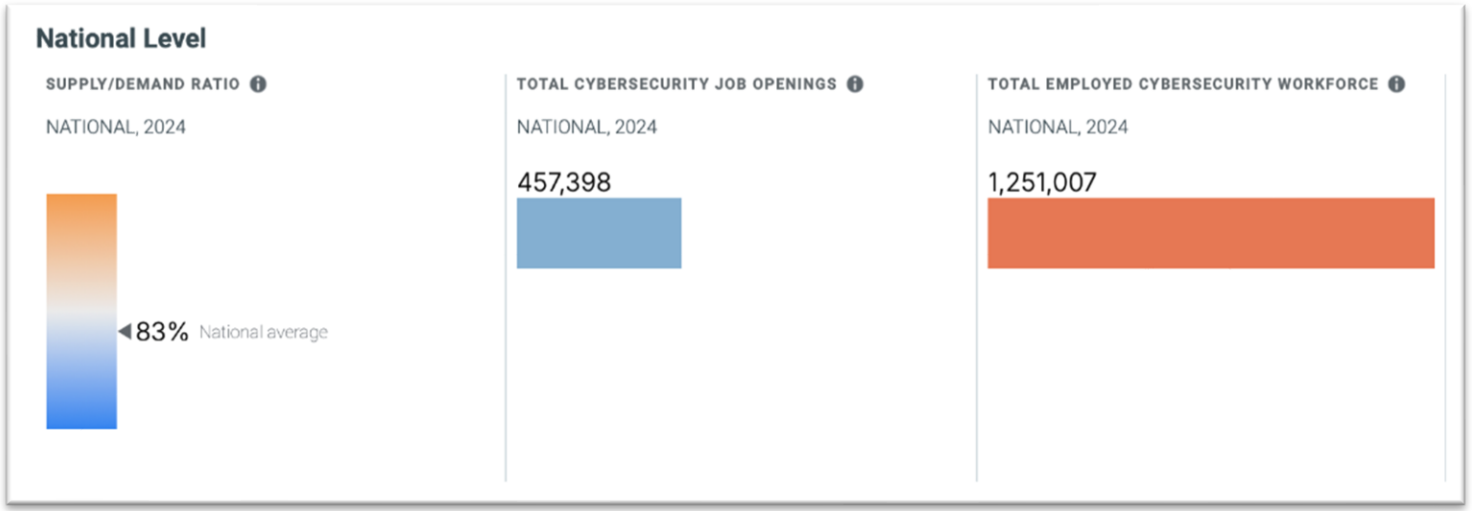
Individuals whose primary focus is on cybersecurity *as well as* those in the workforce who need specific cybersecurity-related knowledge and skills to perform their work.

New Cyberseek Data (10/15/24)

CyberSeek™
www.cyberseek.org

- Nearly 265,000 more cybersecurity workers needed to close current US supply gap
- Cybersecurity workforce has expanded each year since 2013
- Sep. 2023 – Aug. 2024: 457,398 cybersecurity job postings
- 1.25 million people currently work in cybersecurity roles
- Enough workers to fill only 83% of the available cybersecurity jobs
- Requirements for AI skills have increased from 6.3% to 7.3%
- Industry sector growth:
  - Services (except public administration): 40%
  - Agriculture, forestry, fishing and hunting (+26.5%)
  - Wholesale trade (+22.5%)
  - Retail trade (+13.9%)
  - Accommodation and food services (+10.86%)

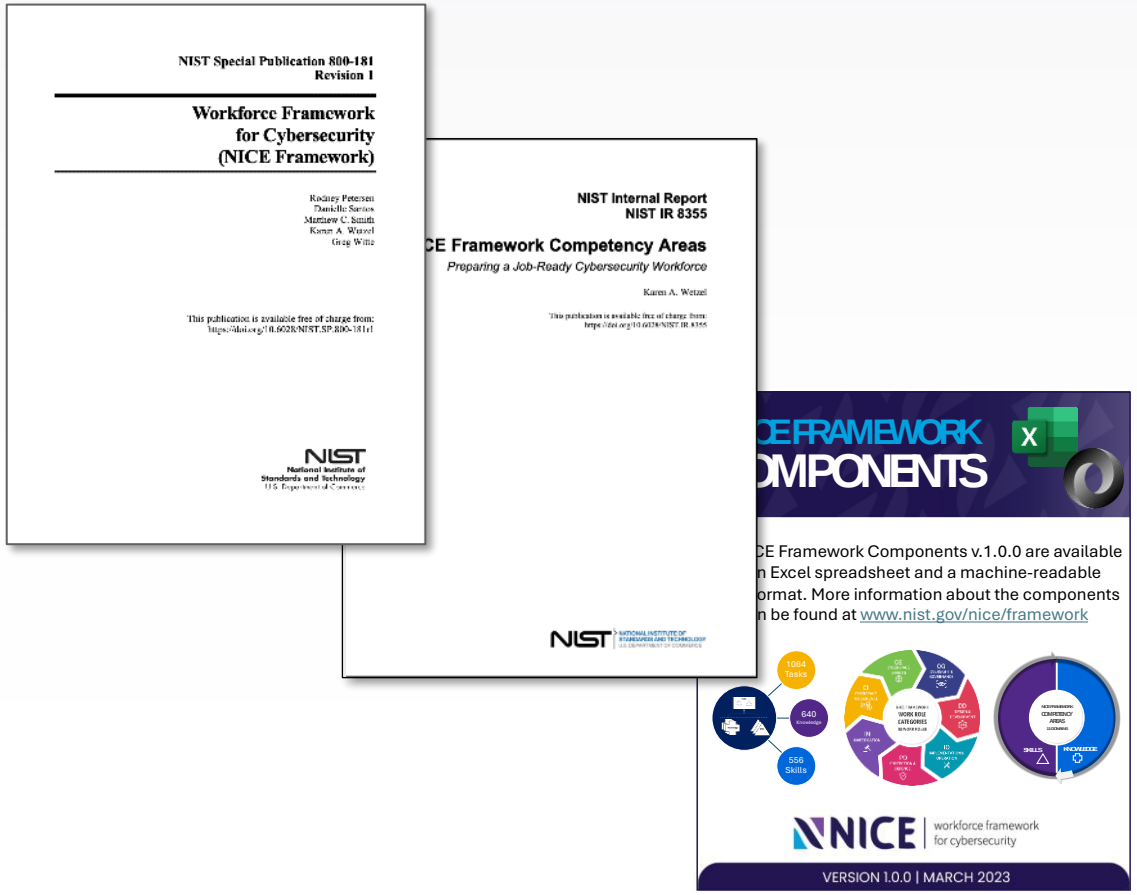




NICE | workforce framework for cybersecurity

NICE Workforce Framework for Cybersecurity (NICE Framework)

NIST SP 800-181r1 (2020) | NISTIR 8355 (2023) | Components v1.0.0 (2024)

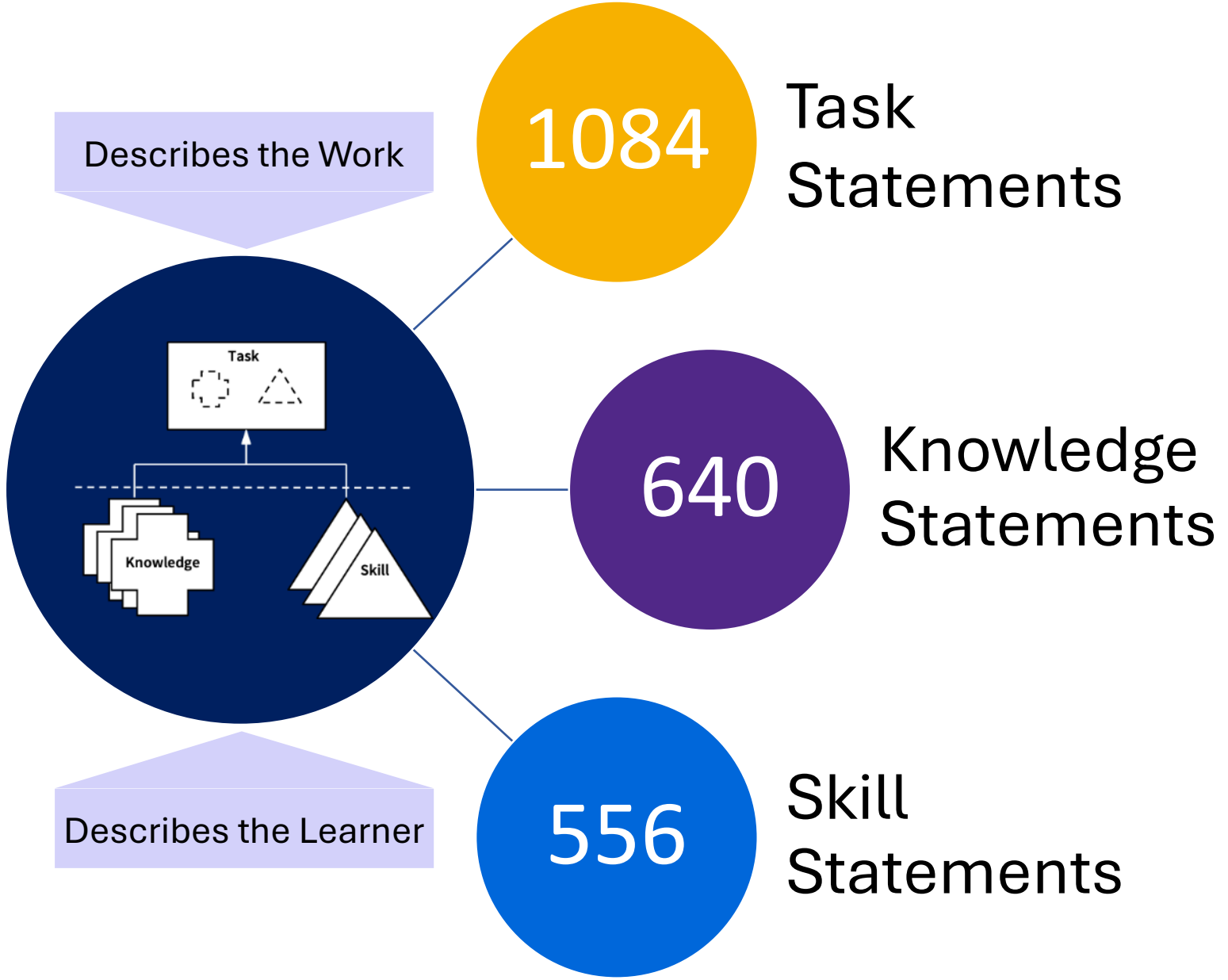


- ✔ A **common language** to clearly share about what a workforce needs to know
- ✔ A **modular, building-blocks approach** based on Task, Knowledge, and Skill (TKS) statements
- ✔ Defined **Work Roles** and **Competency Areas** for use in:
  - Career discovery
  - Education and training
  - Workforce planning and assessment
  - Hiring and career development

TKS Statements

TKS Definitions

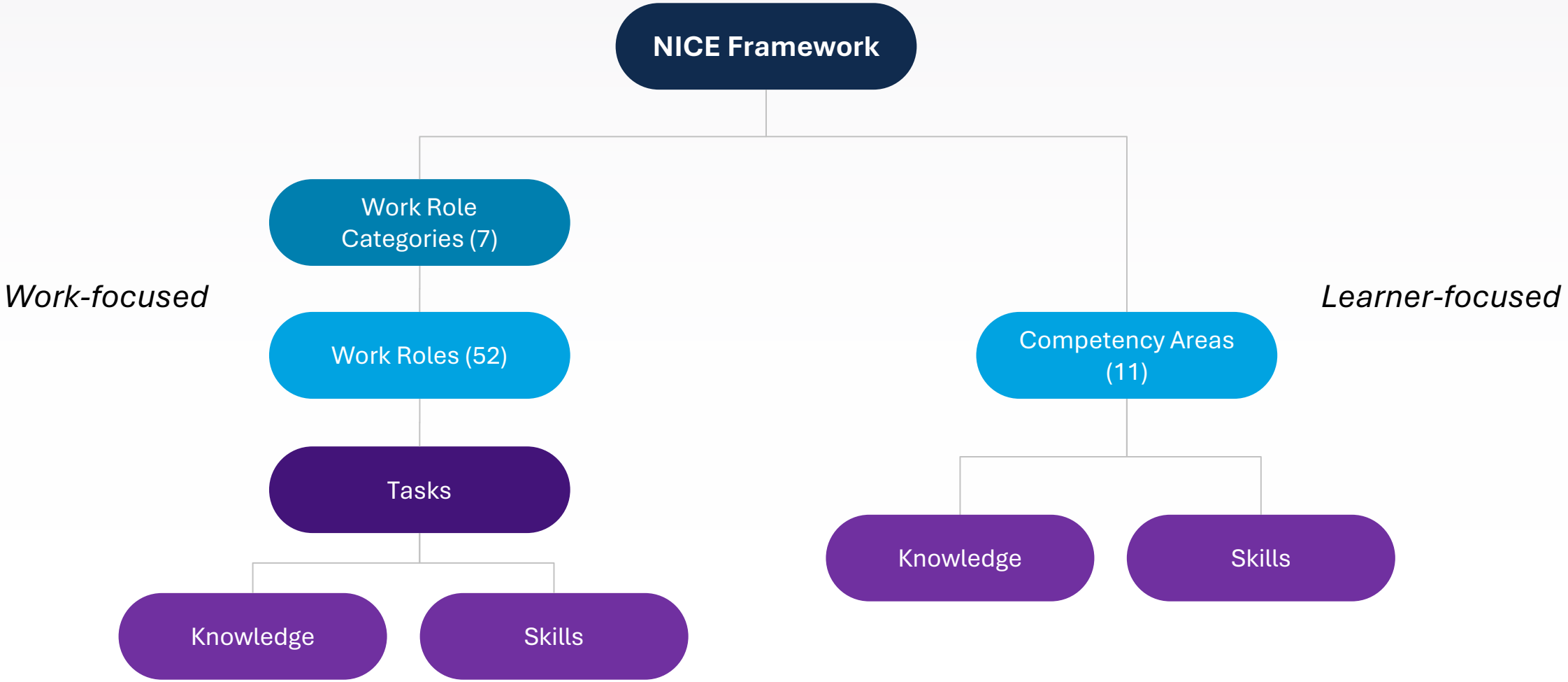
- **Task:** An activity that is directed toward the achievement of organizational objectives.
- **Knowledge:** A retrievable set of concepts within memory.
- **Skill:** The capacity to perform an observable action.



NIST | NICE

Resource: NICE Framework Current Version

NICE Framework Structure



NICE workforce framework for cybersecurity

Resource: Getting Started with the NICE Framework

Credit: NICE

7 Work Role Categories
52 Work Roles

Image source: shutterstock.com

- OVERSIGHT & GOVERNANCE
- DESIGN & DEVELOPMENT
- IMPLEMENTATION & OPERATION
- PROTECTION & DEFENSE
- INVESTIGATION
- CYBERSPACE INTELLIGENCE
- CYBERSPACE EFFECTS

NICE | workforce framework for cybersecurity

Work Role Examples

Work Role Category: Protection and Defense (PD) Protects against, identifies, and analyzes risks to technology systems or networks. Includes investigation of cybersecurity events or crimes related to technology systems and networks.	**Work Role Category: Implementation and Operation (IO)** Provides implementation, administration, configuration, operation, and maintenance to ensure effective and efficient technology system performance and security.
Vulnerability Analysis PD-WRL-007 | OPM Code: 541	**Database Administration** IO-WRL-002 | OPM Code: 421
Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effectiveness of defense-in-depth architecture against known vulnerabilities.	Responsible for administering databases and data management systems that allow for the secure storage, query, protection, and utilization of data.
• 15 Task statements • 64 Knowledge Statements • 18 Skill statements	• 14 Task statements • 57 Knowledge Statements • 14 Skill statements

Example TKS >

T0422	Implement data management standards, requirements, and specifications
T1069	Evaluate organizational cybersecurity policy regulatory compliance
K1014	Knowledge of network security principles and practices
K0919	Knowledge of Personal Health Information (PHI) data security standards and best practices
S0578	Skill in evaluating security designs
S0545	Skill in designing data storage solutions

NIST | NICE

NICE Framework Competency Areas

Competency Area: A cluster of related Knowledge and Skill statements that correlates with one's capability to perform Tasks in a particular domain.

Example:

Cloud Security: This Competency Area describes a learner's capabilities to protect cloud data, applications, and infrastructure from internal and external threats.

Resource: NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce

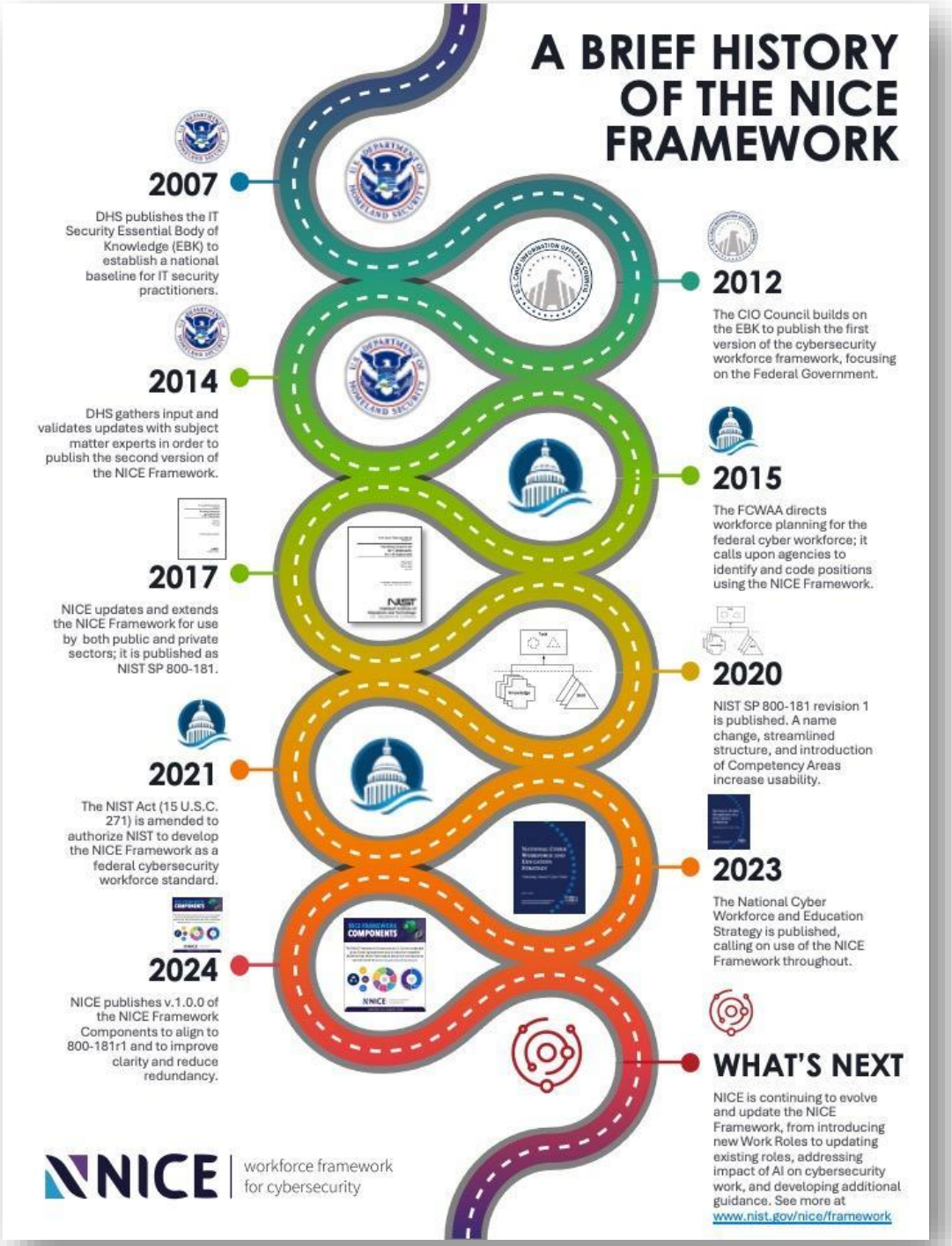
- Access Controls
- Artificial Intelligence (AI) Security
- Asset Management
- Cloud Security
- Communications Security
- Cryptography
- Cyber Resiliency
- DevSecOps
- Operating Systems (OS) Security
- Operational Technology (OT) Security
- Supply Chain Security

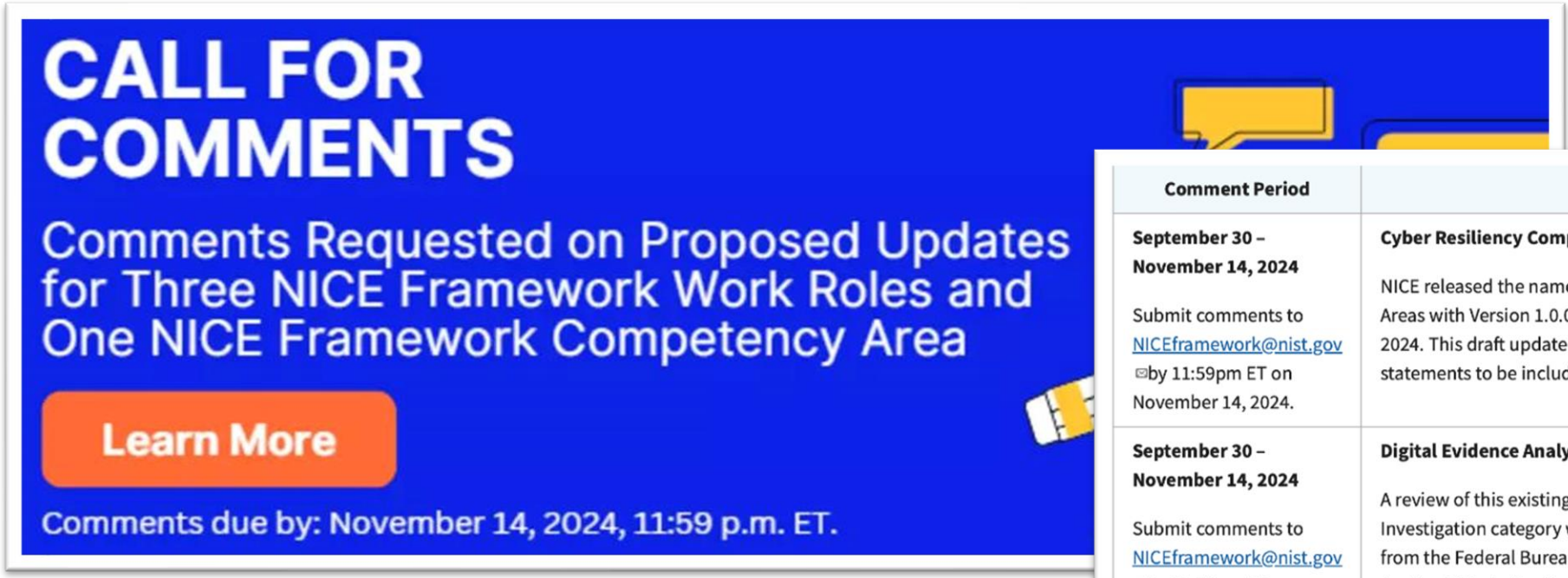
NIST | NICE

Development Process

- Consultative & Open
- Communication & Outreach
- Continuous Improvement
- Update Types:
  - Major (structural, content removal)
  - Minor (additive)
  - Administrative (errata)
- Resources & Appropriation

Resource: NICE Framework Revisions





www.nist.gov/nice/framework

Comment Period	Description	Links
September 30 – November 14, 2024 Submit comments to NICEframework@nist.gov by 11:59pm ET on November 14, 2024.	**Cyber Resiliency Competency Area (NF-COM-007)** NICE released the names and descriptions of 11 new Competency Areas with Version 1.0.0 of the NICE Framework Components in March 2024. This draft update contains proposed Knowledge and Skill statements to be included in the Cyber Resiliency Competency Area.	NF-COM-007 Public Comment Spreadsheet
September 30 – November 14, 2024 Submit comments to NICEframework@nist.gov by 11:59pm ET on November 14, 2024.	**Digital Evidence Analysis Work Role (IN-WRL-002)** A review of this existing NICE Framework Work Role in the Investigation category was conducted with subject matter experts from the Federal Bureau of Investigation and the Department of Justice. This draft adjusts the Task, Knowledge, and Skill statements in this Work Role and aligns Knowledge and Skill statements to each Task.	IN-WRL-002 Public Comment Spreadsheet
September 30 – November 14, 2024 Submit comments to NICEframework@nist.gov by 11:59pm ET on November 14, 2024.	**Insider Threat Analysis Work Role (PD-WRL-005)** This Work Role was initially released with Version 1.0.0 of the NICE Framework Components in March 2024. This update includes minor changes to some Task, Knowledge, and Skill statements and aligns the Knowledge and Skill statements to each Task statement in this role.	PD-WRL-005 Public Comment Spreadsheet
September 30 – November 14, 2024 Submit comments to NICEframework@nist.gov by 11:59pm ET on November 14, 2024.	**Operational Technology (OT) Cybersecurity Engineering Work Role (New DD-WRL-009)** This new Work Role in the NICE Framework Design & Development Work Role Category is the first role in the NICE Framework to focus on operational technology (OT).	DD-WRL-009 Public Comment Spreadsheet

In Development:

- AI Security Competency Area
- Supply Chain Security Competency Area
- Risk Management Work Role
- Learning Program Management Work Role

Forthcoming:

- Product Security
- Cloud Security
- Facilities Management
- And more

NICE | workforce framework for cybersecurity

Image source: shutterstock.com

Example Use: Hiring

Common Challenges

Unclear workforce needs

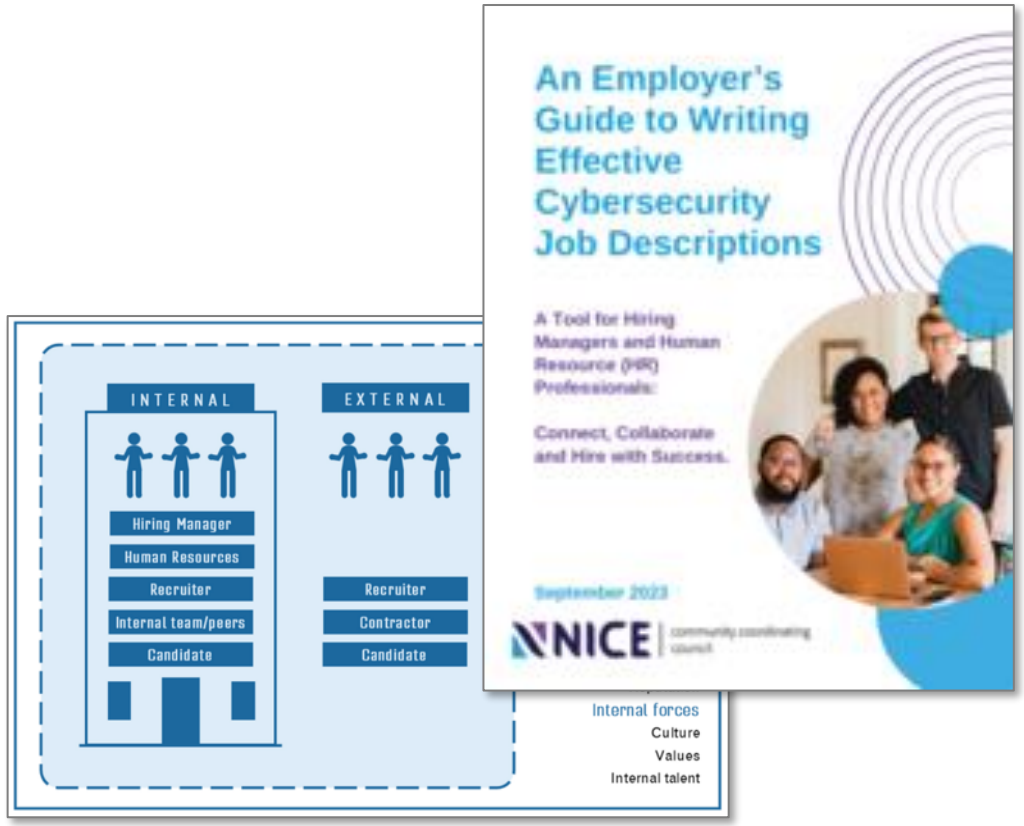
Working without a detailed position description

Conducting a candidate search with unrealistic goals

Employer's Guide (2023)

Three-step Approach:

1. Define Hiring Criteria
2. Define the Job
3. Candidate Assessment



Hiring Ecosystem

Community, environment, and the resulting interconnections needed to recruit employees into an organization. Includes:

- Human components
- Institutional processes
- Different technologies

Resource: NICE Modernize Talent Management Working Group

Creating Position Descriptions

- Hiring Managers & HR work together
- Identify relevant Work Role(s)
- Confirm appropriate tasks, knowledge, and skills
- Determine requirements
- Reference roles and tasks in PD

Candidate Assessment	0-1	2-3	4-5	Total
T0124 Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts).			Required: 5	
K0086 Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.		Required: 3		
S0001 Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.		Required 3		

NIST | NICE

USAJobs Examples

Information Technology Specialist (Security)

JUDICIAL BRANCH

Administrative Office of the U.S. Courts

IT Security Office, Security Operations Division

judiciary.

8. Documenting and communicating with all internal and external stakeholders to ensure relevant data is provided for sound decision-making and situational awareness.
9. Understanding attack signatures, tactics, techniques, and procedures associated with advanced threats. .
10. The incumbent of this position must be able to perform the tasks and meet the skills, knowledge and abili described in NIST Special Publication 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework for the roles of Cyber Crime Investigator (IN-INV-001) and Cyber Defer Forensics Analyst (IN-FOR-002).

IT Cybersecurity Specialist (INFOSEC)

DEPARTMENT OF VETERANS AFFAIRS

Deputy Assistant Secretary for Information and Technology

Office of Information and Technology, Infrastructure Operations, IO Cybersecurity Management

Duties

This is a non-bargaining unit position.

The initial application review cut-off for this job announcement is 50 applications. the first 50 applications received will be considered first. Applications received after the initial cut-off number (50 applications) may not receive consideration unless otherwise requested by management. If management requests additional certificates, applicants will continue to be reviewed in groups of 50 in the order they applied.

This position is primarily aligned to the following NICE Cybersecurity Workforce Framework work roles:

- 461 Systems Security Analyst

For more information about these work roles, where they fit within the larger Cyber Workforce, and how they can

https://cybersecurity.usajobs.gov/job/756222600
https://www.usajobs.gov/job/746332400

NIST | NICE

Image source: shutterstock.com

Example Use: Career Development

Career Pathways

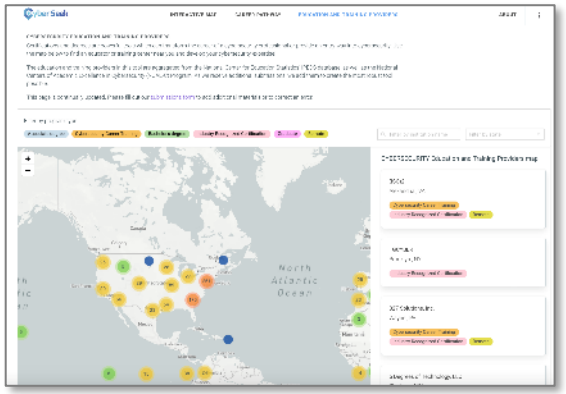
Upskilling & Reskilling

Demonstrating Capability

NIST | NICE

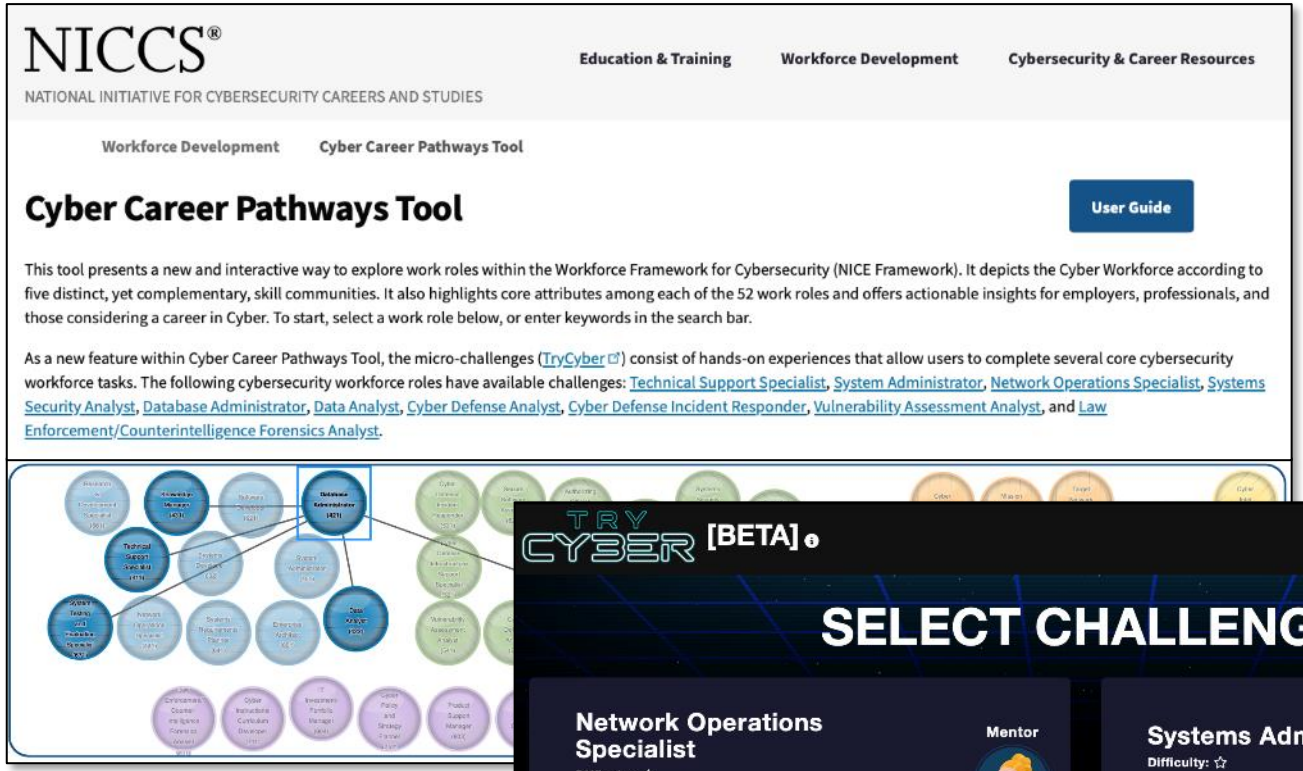
Cybersecurity Education & Training

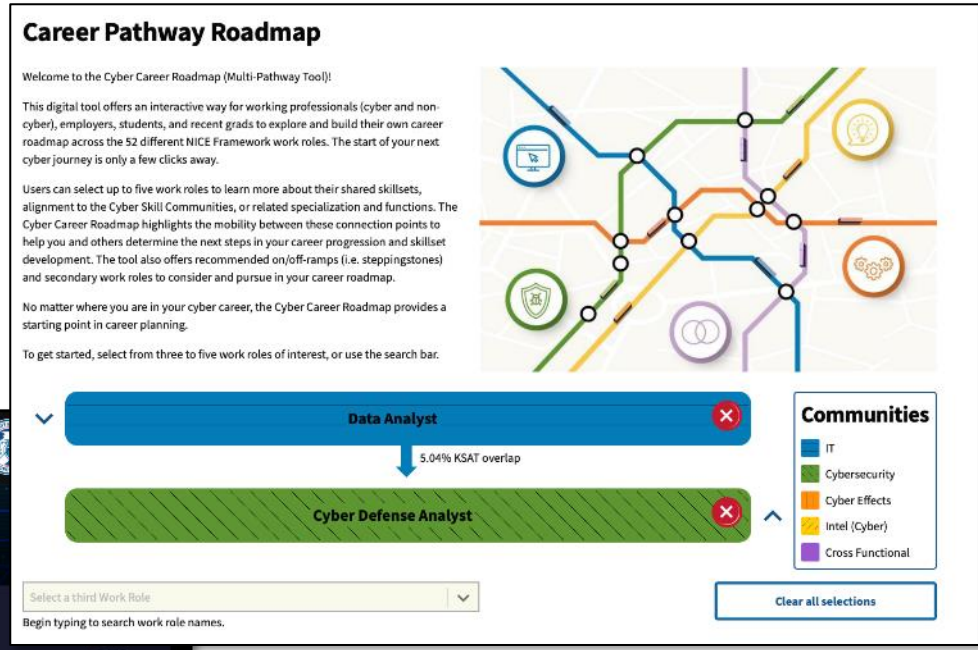
- NICE Free and Low Cost Online Cybersecurity Learning Content
  - Career and Professional Development
  - Employee Awareness Training
  - Educator Training and Curriculum
  - K12 Education and Games
- NICCS Education & Training Catalog
- CyberSeek Cybersecurity Education and Training Providers
- Cybersecurity Credentials Collaborative (C3) Certifications Mapping to NICE Framework
- FedVTE (Federal Virtual Training Environment)
- CLARK Center



NIST | NICE

NICCS Cyber Career Pathway Tool





https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool

https://trycyber.us/

NIST | NICE

CyberSeek Career Pathways

Cybersecurity Analyst

AVERAGE SALARY

$107,346

COMMON JOB TITLES

- Information Security Analysts
- Cybersecurity Analysts
- IT Security Analysts
- Security Operations Analysts
- Security Operations Center Analysts

REQUESTED EDUCATION (%)

TOTAL JOB OPENINGS

25,571

TOP FUTURE SKILLS REQUESTED

Skills	5-Year Projected Growth
Public Cloud Security	121%
Comprehensive Software Security	114%
Threat Hunting	105%
Security Information and Event Management (SIEM)	65%
Threat Intelligence & Response	53%

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

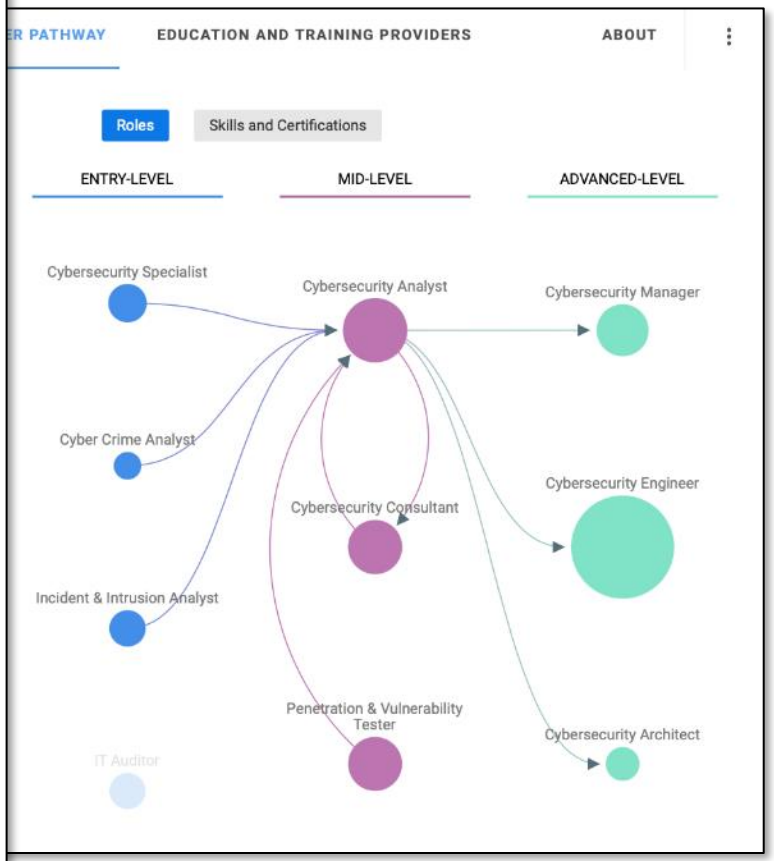
- Securely Provision
- Operate and Maintain
- Protect and Defend
- Analyze
- Investigate
- Oversee and Govern
- Collect and Operate

TOP CERTIFICATIONS REQUESTED

- Certified Information Systems Security Professional
- GIAC Certifications
- CompTIA Security+
- Certified Information System Auditor (CISA)
- Certified Information Security Manager

TOP SKILLS REQUESTED

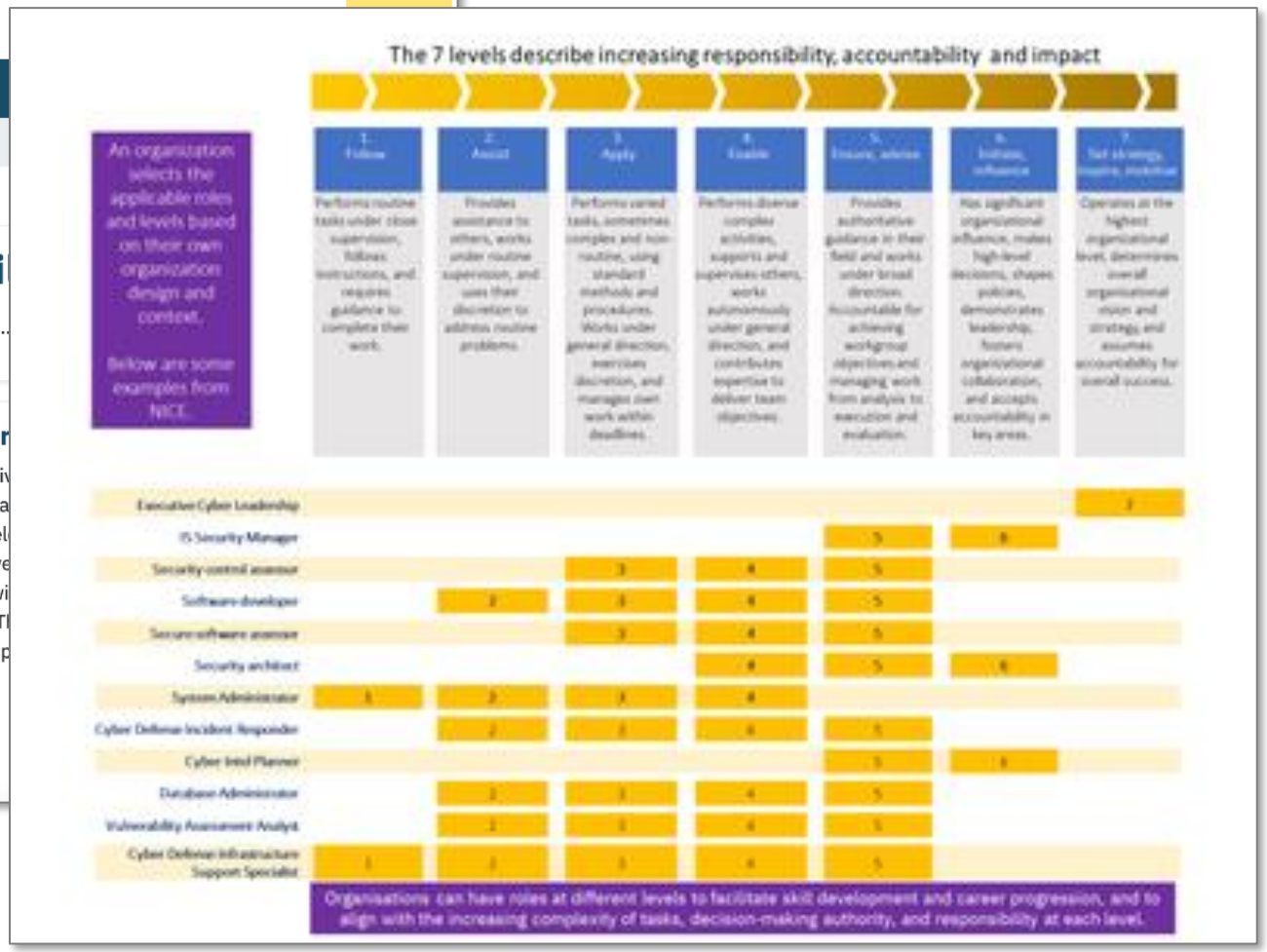
1. Cyber Security
2. Vulnerability
3. Computer Science
4. Auditing
5. Incident Response
6. Risk Analysis
7. Information Systems
8. Security Controls
9. Security Information And Event Management (SIEM)



NIST | NICE

www.cyberseek.org

SFIA Mapping to NICE Work Roles



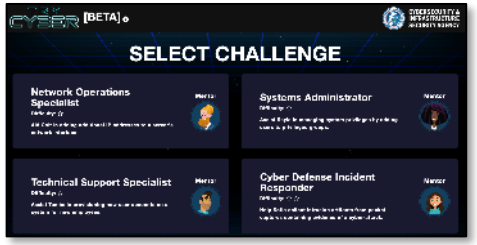
https://sfia-online.org/en/tools-and-resources/sfia-views/sfia-view-information-cyber-security/mapping-nice-work-roles-to-sfia-skills

NIST | NICE

Use & Adoption

- **TKS usage**
  - US Cyber Games, NICE Challenge Project, TryCyber.us, President's Cup
  - CAE Community, CLARK.center
  - C3 Certification Mappings
- **Career discovery and pathways**
  - Cyberseek.org
  - NICCS Career Pathways Tool
  - SFIA
  - NICE K12, Apprenticeships
  - USAJobs, MilGears, Cybercareers.gov
- **Create job descriptions and assess candidates**
  - Employers Guide to Writing Job Descriptions
  - CAE Competency Model
  - DHS PushButton Tool
- **Track and plan workforce capabilities**
  - NICE Framework Success Stories
  - Community Coordinating Council Calls
- **Research & Data**
  - OPM Cyber Workforce Dashboard
  - LinkedIn Economic Graph, SANS GIAC Report
- **Playbook for Workforce Frameworks & International Use**

GOVERNMENT • INDUSTRY • NONPROFIT • ACADEMIA



NICE | workforce framework for cybersecurity

Additional Resources

www.nist.gov/nice/framework

NICE Framework Resource Center

- Getting Started & FAQs
- Documents & Data - Web version, XLXS, JSON, CTDL, & Translations
- Public Comments, Change Request FAQs, Change Logs
- Playbook for Workforce Frameworks & Authoring Guides
- Success Stories (Case Studies) and Framework in Focus (Practitioner Interviews)
- Employer, Educator, Learner, and International Resources
- Employers Guide to Developing Job Descriptions
- Workplace Skills
- Users Group

NICE Framework Tools

- CyberSeek: An interactive cybersecurity jobs heat map across the U.S. by state and metropolitan areas and career pathway tool.
- NICE Framework Tool & Keyword Search: Enables browsing and searching.
- NICE Framework Mapping Tool: Answer questions about your federal cybersecurity-related position and the tool will show you how it aligns to the NICE Framework and what can be done to strengthen your cybersecurity team.
- NICCS Education and Training Catalog: Cybersecurity professionals across the nation can find over 6,000 cybersecurity-related courses aligned with the NICE Framework.
- NICCS Cyber Career Pathways Tool: Includes common relationships between roles as well as frequently used titles in each role. (Federal)
- NICE Challenge Project: Real-world cybersecurity challenges within virtualized business environments to provide students with workforce experience before entering the workforce.

HIPAA Compliance and Enforcement Updates

Emily Crabbe, Senior Advisor for HIPDC
Compliance and Enforcement

Office for Civil Rights (OCR)
U.S. Department of Health and Human Services

OCR/NIST Conference

October 24, 2024

HIPAA Priorities

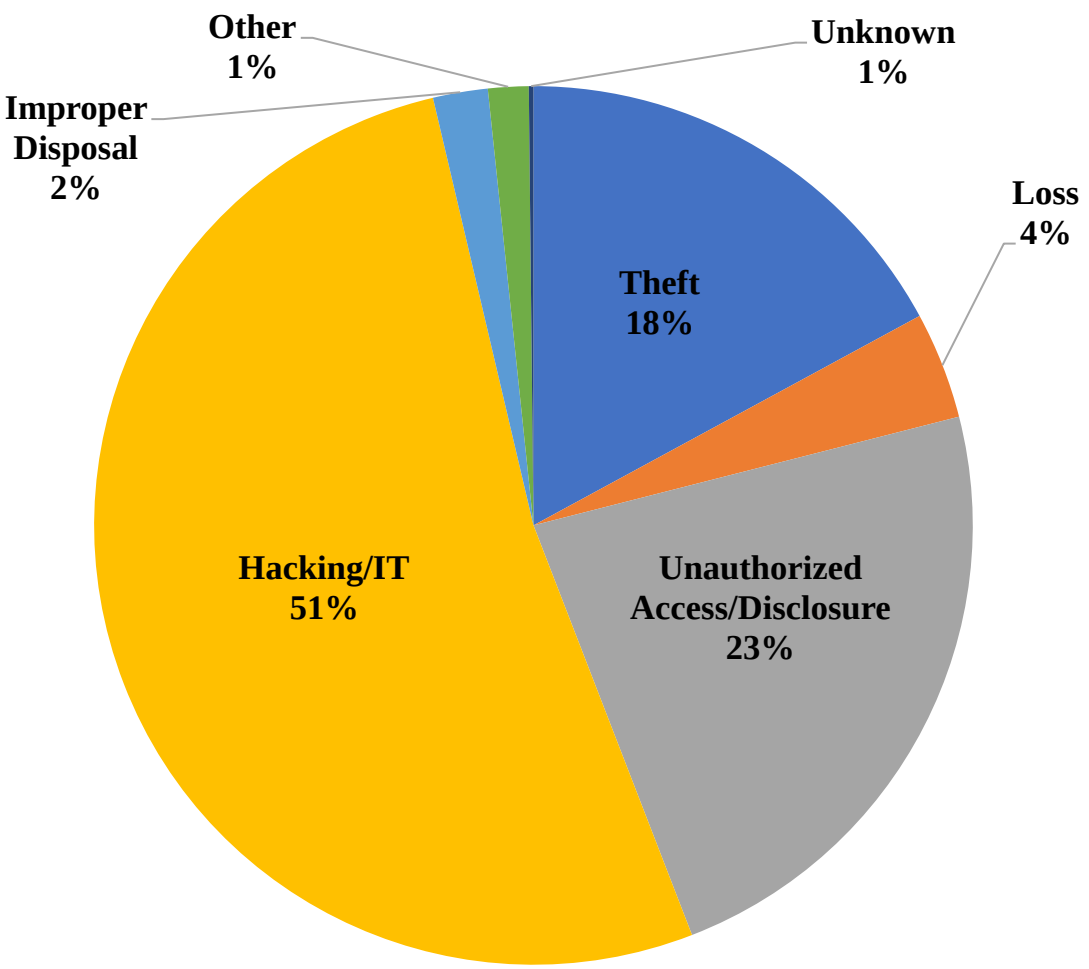
- Prioritizing investigations that follow HIPAA complaint and breach trends:
  - Hacking
  - Ransomware
  - *Right of Access Enforcement Initiative*
  - *Risk Analysis Enforcement Initiative*
- Engaging with Health Care Industry on Cybersecurity
  - Increased presence regionally across the country
  - Videos/Guidance/Newsletters
  - Webinars/Technical Assistance
- Review and Update HIPAA Security Rule

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

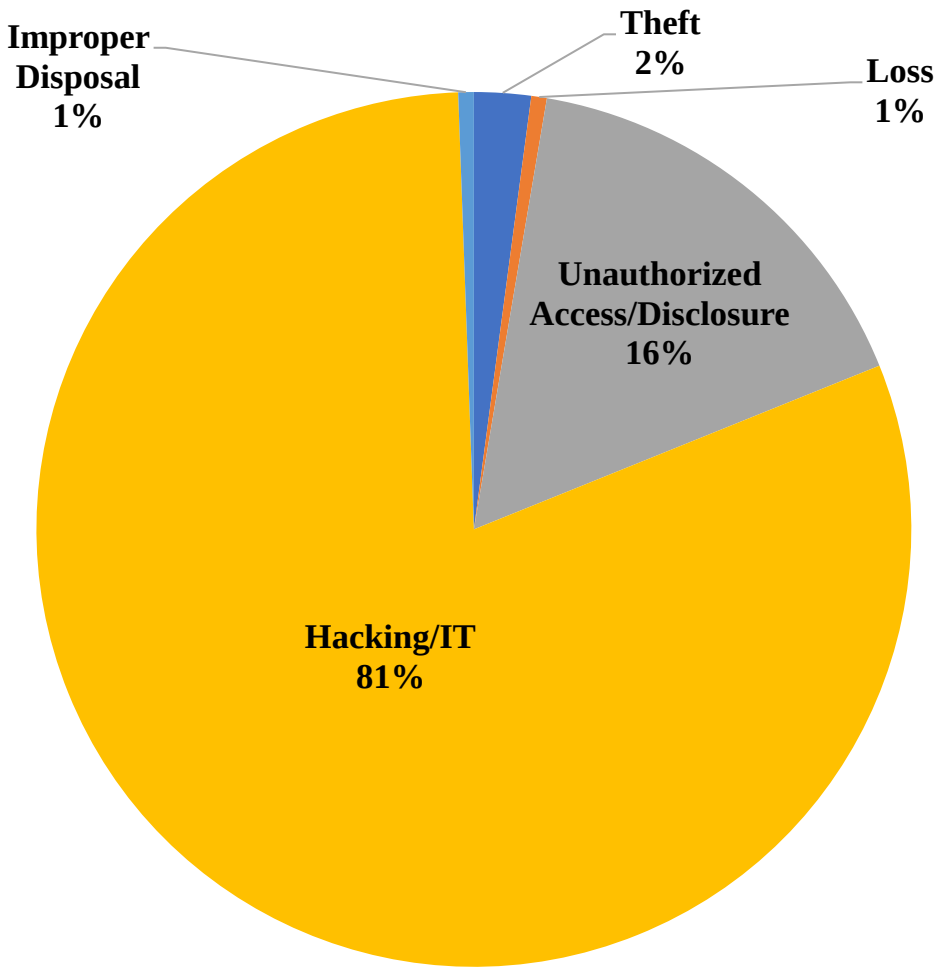
What Happens When OCR Receives a Breach Report

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
  - Received over 700 breach reports affecting 500+ individuals in 2023
- OCR opens investigations into breaches affecting 500+ individuals, and into a number of smaller breaches
- OCR breach investigations examine:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (breach notification) and prevent future incidents
  - Entity's compliance prior to the breach

500+ Breaches by Type of Breach

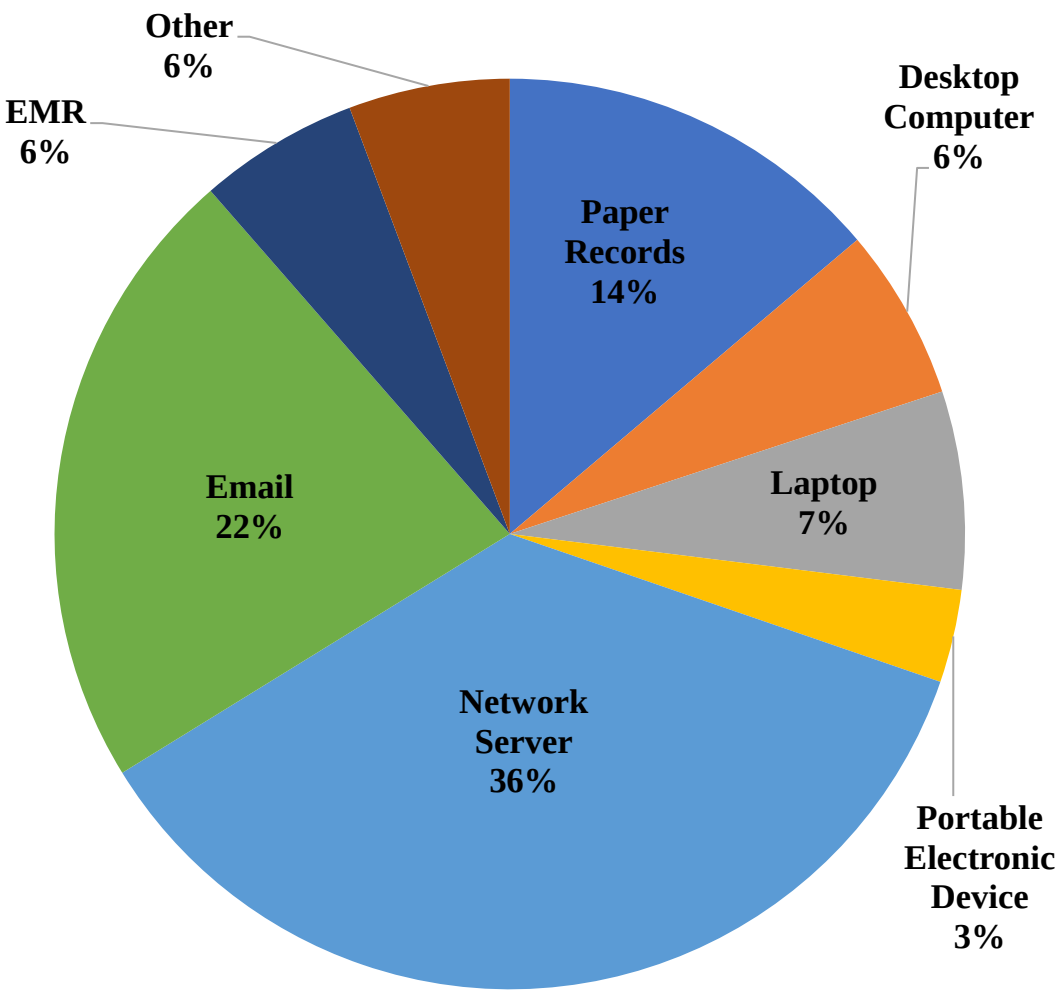


September 23, 2009 through Dec 31, 2023

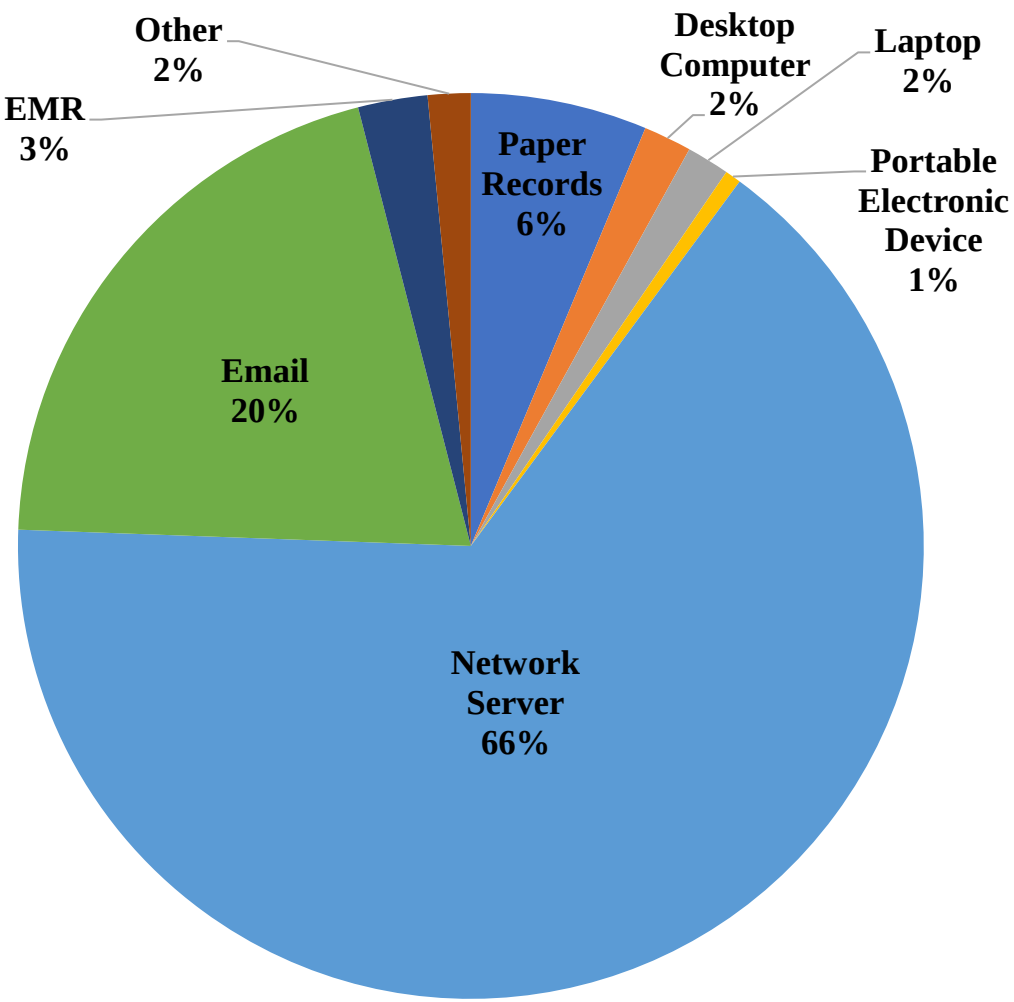


January 1, 2024 through September 30, 2024

500+ Breaches by Location of Breach



September 23, 2009 through Dec 31, 2023

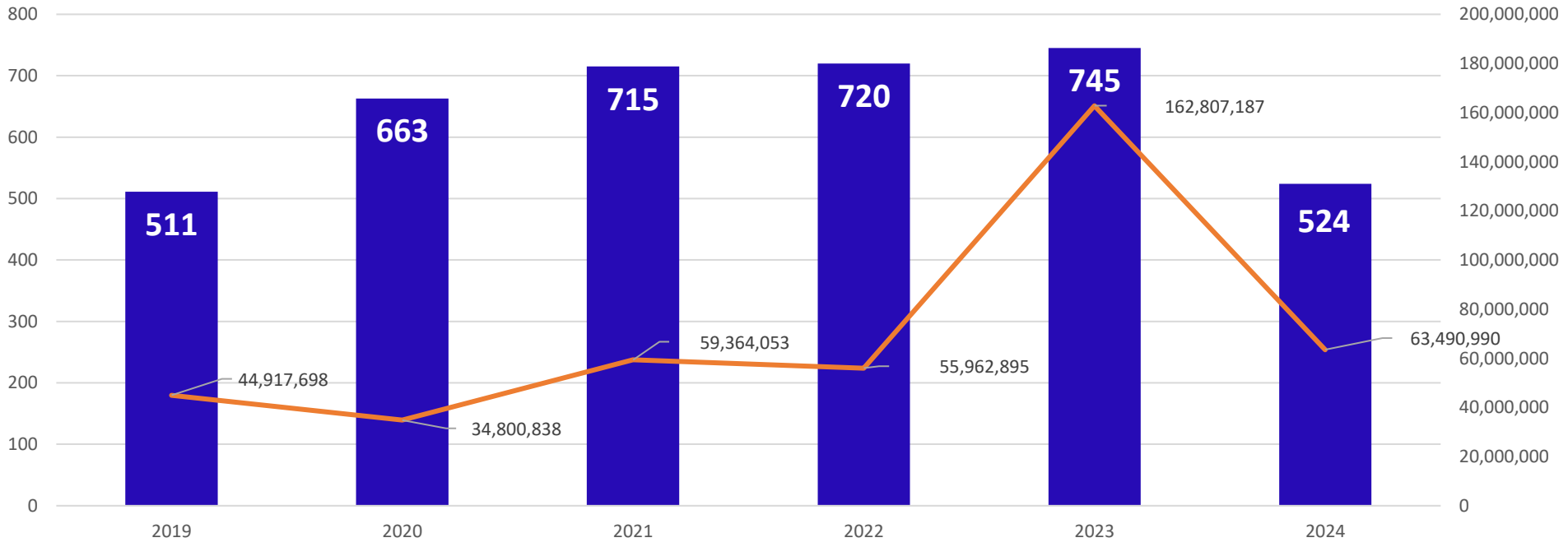


January 1, 2024 through September 30, 2024

Breaches Affecting 500 or More Individuals

Reports Received and Individuals Affected

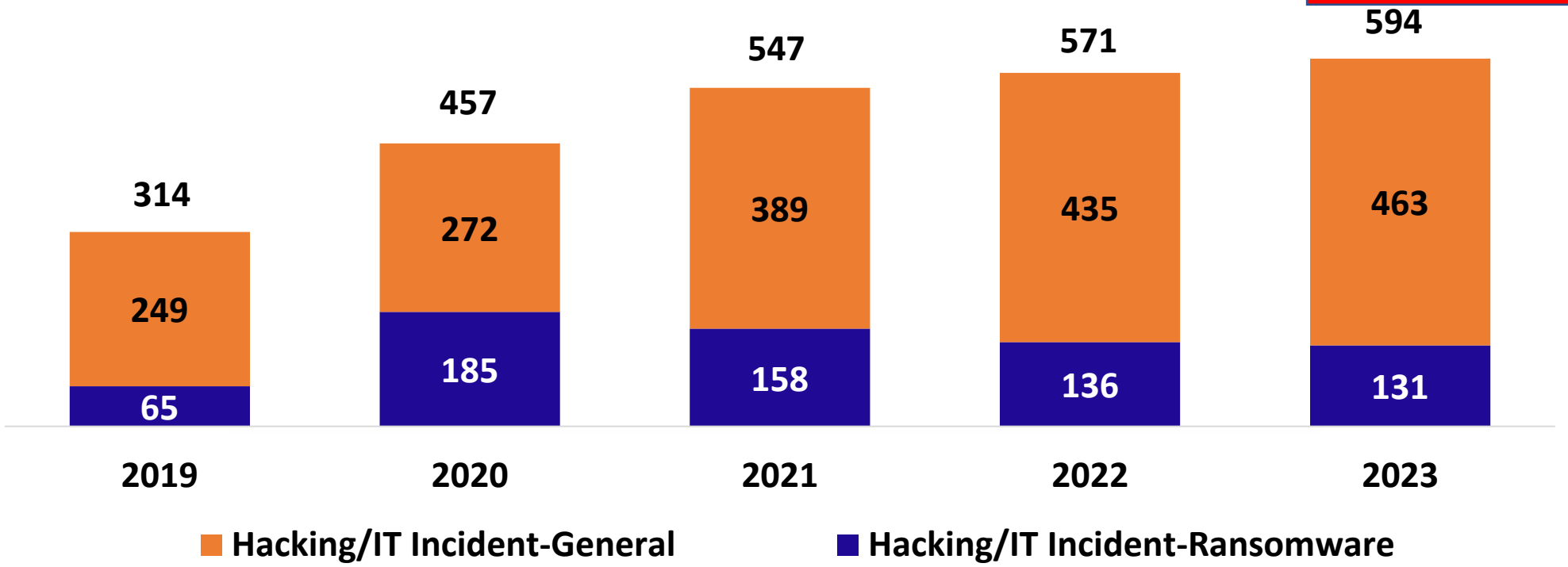
Calendar Years 2019 – August 2024



Breaches Affecting 500 or More Individuals
Reports Received Involving Hacking/IT Incidents

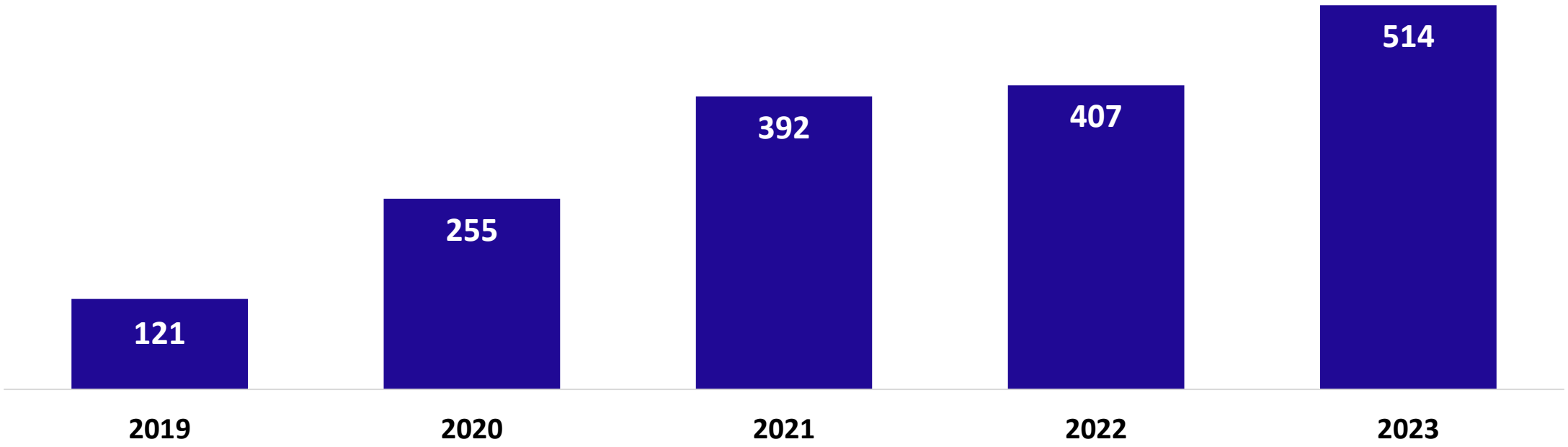
Calendar Years 2019 - 2023

2019 - 2023
89% increase in hacking
102% increase in ransomware



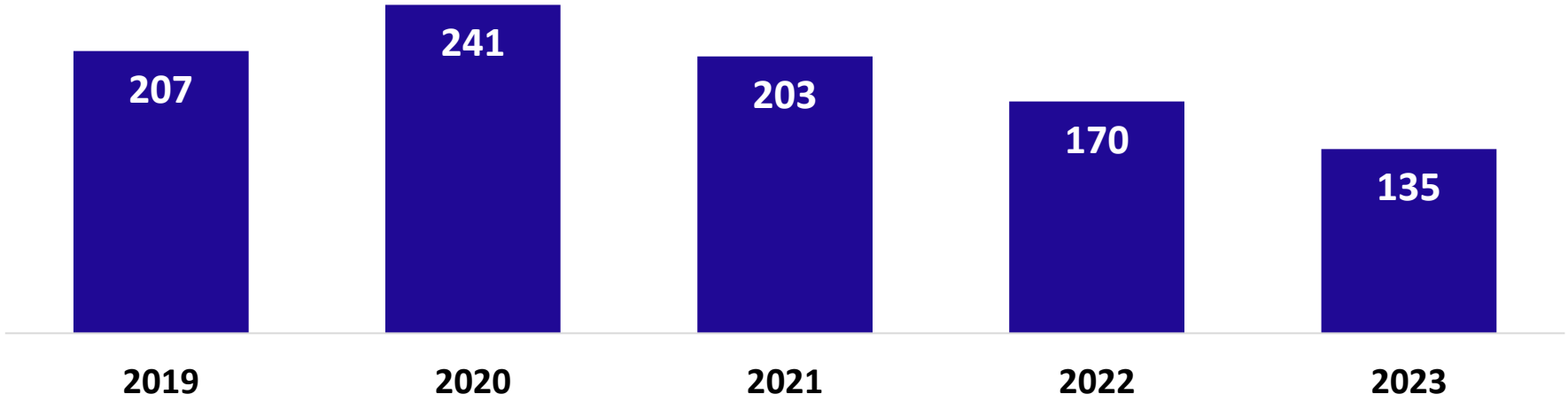
Breaches Affecting 500 or More Individuals
Reports Received of Breaches Involving Network Servers

Calendar Years 2019 - 2023



Breaches Affecting 500 or More Individuals
Reports Received of Breaches Involving Email Accounts

Calendar Years 2019 - 2023



Recurring HIPAA Compliance Issues

- Individual Right of Access
- Risk Analysis
- Business Associate Agreements
- Access Controls
- Audit Controls
- Information System Activity Review

General HIPAA Enforcement Highlights (Aug 2024)

- OCR received 31,731 HIPAA cases in 2023.
- In most cases, entities are able to demonstrate satisfactory compliance through voluntary cooperation and corrective action.
- In some cases, the nature or scope of indicated noncompliance warrants additional enforcement action.
- Resolution Agreements/Corrective Action Plans
  - 139 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 10 civil money penalties

Recent Announced OCR HIPAA Enforcement Actions

Heritage Valley Health System	$950,000
Cascade Eye & Skin	$250,000
Providence Medical Institute	*$240,000
Montefiore Medical Center	$4,750,000
Lafourche Medical Group	$480,000
Green Ridge Behavioral Health, LLC	$40,000
Doctors' Management Services	$100,000
LA Care Health Plan	$1,300,000
Yakima Valley Memorial Hospital (formerly Virgina Mason)	$240,000
iHealth Solutions, LLC	$75,000
MedEvolve, Inc.	$350,000

Best Practices

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Dispose of PHI on media and paper that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy and security

Risk Analysis Initiative

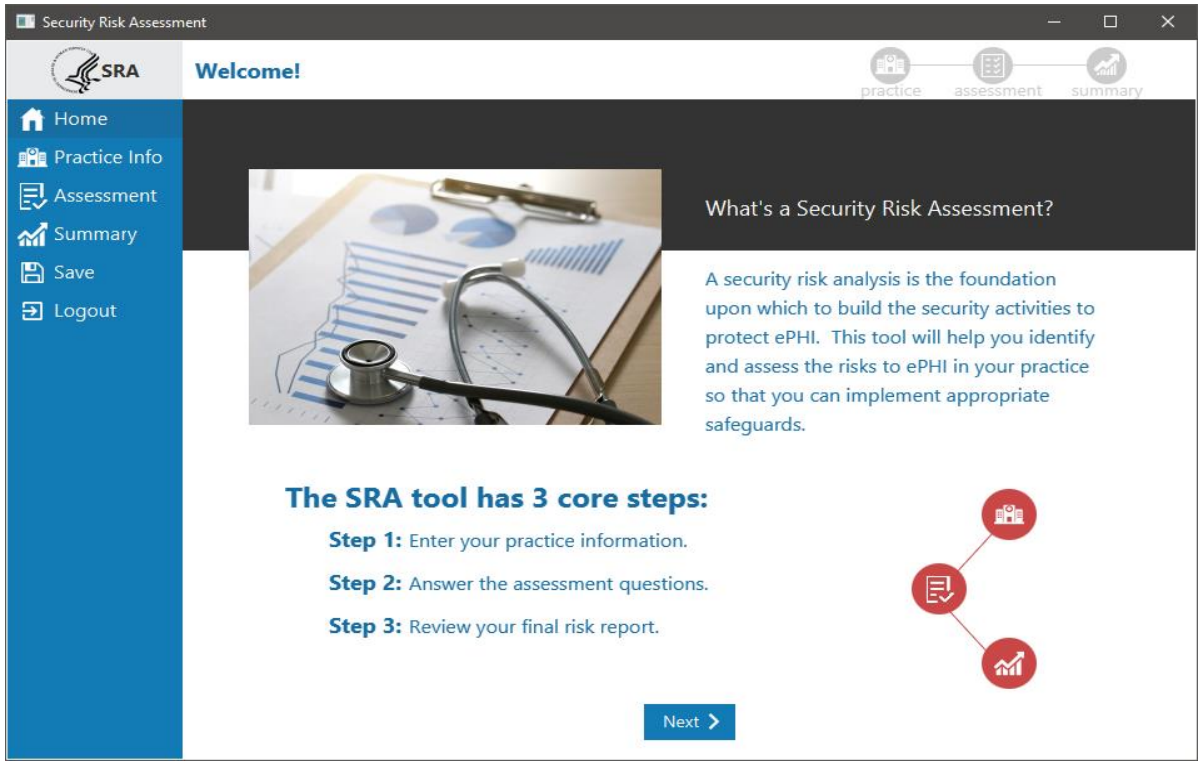
- New Enforcement Initiative
- Focus on compliance with key HIPAA Security Rule requirement
- Most OCR large breach investigations reveal a lack of a compliant risk analysis
- Drive better practices to protect electronic protected health information (ePHI)
- Better overall security of data

OCR HIPAA Risk Analysis Webinar

- Video on the HIPAA Security Rule Risk Analysis requirement.
- Discusses what is required to conduct an accurate and thorough assessment of potential risks and vulnerabilities to ePHI and review common risk analysis deficiencies OCR has identified in investigations.
- Topics covered include:
  - How to prepare for a risk analysis
  - How should ePHI be assessed
  - What does it mean to be accurate and thorough
  - What purpose does a risk analysis serve once completed
  - Examples from OCR investigations
  - Resources

The video may be found on OCR's YouTube channel at: https://www.youtube.com/watch?v=hxfxhokzKEU

SRA Tool



https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

Designed to assist small to medium sized organizations in conducting an internal security risk assessment to aid in meeting the security risk analysis requirements of the HIPAA Security Rule and the CMS EHR Incentive Program.

The SRA tool guides users through a series of questions based on standards identified in the HIPAA Security Rule. Responses are sorted into Areas of Success and Areas for Review.

Not all areas of risk may be captured by the tool. Risks not identified and assessed via the SRA Tool must be documented elsewhere.

HITECH Amendment on Recognized Security Practices and Video

- 2021 HITECH Amendment requires OCR to consider whether a regulated entity has adequately demonstrated that recognized security practices were “in place” for the prior 12 months.
- Can mitigate civil money penalties, other remedies in settlement agreements, or early, favorable termination of audits.
- No liability for electing not to implement recognized security practices.
- OCR published a video in October 2022 that covers:
    - The 2021 HITECH Amendment
    - How regulated entities can adequately demonstrate that RSPs are in place
    - How OCR is requesting evidence of RSPs
    - Resources for information about RSPs
    - OCR’s 2022 Request for Information on RSPs
- The video may be found on OCR’s YouTube channel at: https://youtu.be/e2wG7jUiRjE

OCR Common Cyber-Attacks Video

- Video on how the HIPAA Security Rule can help regulated entities defend against common cyber-attacks
- Topics covered include:
  - OCR breach and investigation trend analysis
  - Common attack vectors
  - OCR investigations of weaknesses that led to or contributed to breaches
  - How Security Rule compliance can help regulated entities defend against cyber-attacks

- The video may be found on OCR's YouTube channel at: http://youtube.com/watch?v=VnbBxxyZLc8
- The video in Spanish may be found on OCR's YouTube channel at: http://youtube.com/watch?v=3oVarCxLcB8

Cybersecurity Newsletters

- Recent Topics Include:
  - Facility Access Controls
  - Sanction Policies
  - Cybersecurity Authentication
  - Security Incident Procedures
  - Defending Against Common Cyber-Attacks
  - Securing Your Legacy [System Security]
  - Controlling Access to ePHI
  - HIPAA and IT Asset Inventories
  - Preventing, Mitigating, and Responding to Ransomware
  - Advanced Persistent Threats and Zero Day Vulnerabilities
- Sign up for the OCR Listserv: http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Ransomware Resources

HHS Health Sector Cybersecurity Coordination Center Threat Briefs:

- https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#sector-alerts

Section 405(d) of the Cybersecurity Act of 2015 Resources:

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients https://405d.hhs.gov/Documents/HICP-Main-508.pdf
- 405(d) Products, Publications and Materials https://405d.hhs.gov/resources

OCR Guidance:

- Ransomware https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
- Cybersecurity https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
- Risk Analysis https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

HHS Security Risk Assessment Tool: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

CISA Resources:

- https://www.cisa.gov/stopransomware
- https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare

FBI Resources:

- https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
- https://www.ic3.gov/Media/Y2019/PSA191002

Connect with Us

Office for Civil Rights

U.S. Department of Health and Human Services

www.hhs.gov/hipaa

Join our Privacy and Security listservs at
https://www.hhs.gov/hipaa/for-professionals/list-serve/

@HHSOCR

Contact Us

Office for Civil Rights

U.S. Department of Health and Human Services

ocrmail@hhs.gov
www.hhs.gov/ocr

Voice: (800) 368-1019
TDD: (800) 537-7697
Fax: (202) 519-3818

200 Independence Avenue, S.W.
H.H.H Building, Room 509-F
Washington, D.C. 20201