

NIST Cybersecurity Framework (CSF) 2.0: Overview & Resources

Cherilyn Pascoe

Director, NIST National Cybersecurity Center of Excellence (NCCoE)

October 2024

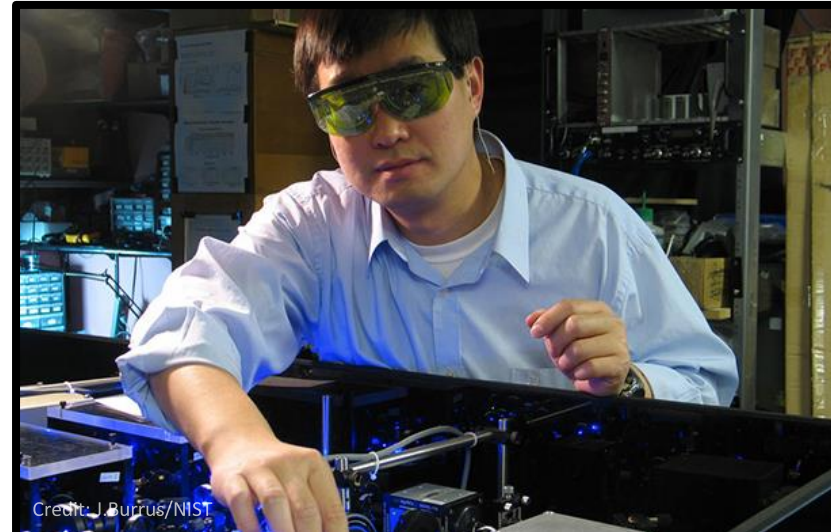
Agenda



- 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

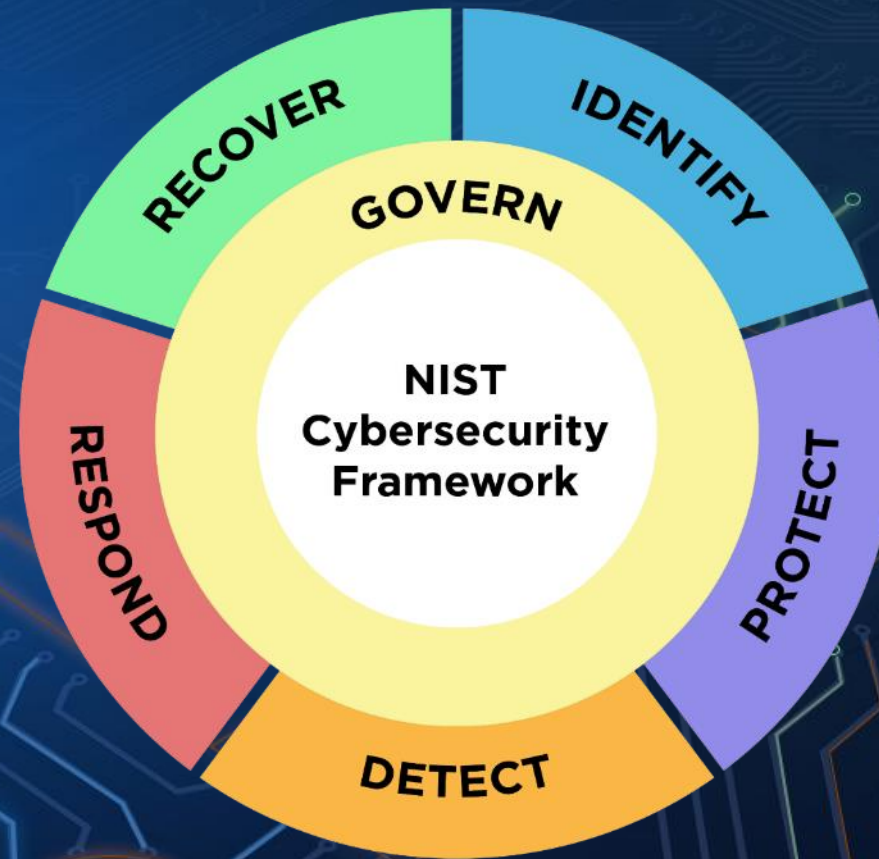
To promote U.S. innovation and industrial competitiveness by advancing **measurement science, standards, and technology** in ways that enhance economic security and improve our quality of life



NIST's Priority Areas in Cybersecurity and Privacy



Brief Overview of CSF 2.0



NIST Cybersecurity Framework

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.





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

The nucleus of the CSF. A **taxonomy of high-level cybersecurity outcomes** that can help any organization manage its cybersecurity risks.

Functions>Categories>Subcategories

CSF Organizational Profiles

A mechanism for describing an organization's **current and/or target cybersecurity posture** in terms of the CSF Core's outcomes.

CSF Tiers

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.

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

Adapted in several countries and regions

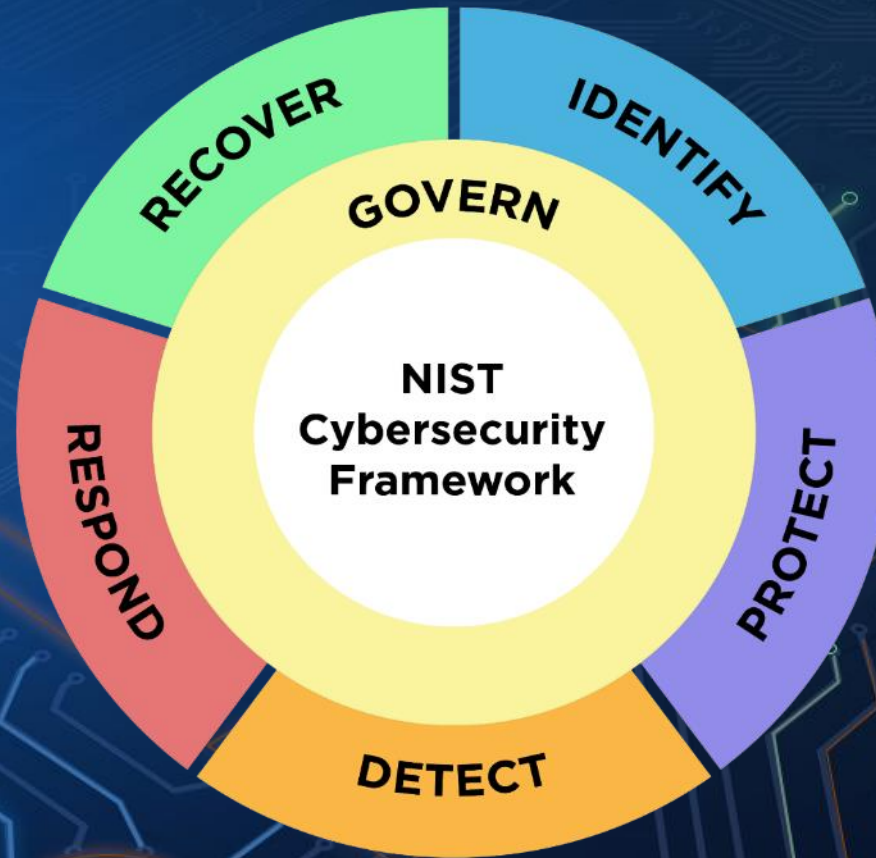
- United States (federal and state)
 - **The White House National Cybersecurity Strategy (March 2023):** <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>
 - “Regulations should be performance-based, leverage existing cybersecurity frameworks, voluntary 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



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?



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

| | |
|---|--|
| 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

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

| Function | Category | Category Identifier |
|-----------------------------|---|---------------------|
| <u>Govern (GV)</u> | 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 |
| <u>Identify (ID)</u> | Asset Management | ID.AM |
| | Risk Assessment | ID.RA |
| | Improvement | ID.IM |
| <u>Protect (PR)</u> | 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 |
| <u>Detect (DE)</u> | Continuous Monitoring | DE.CM |
| | Adverse Event Analysis | DE.AE |
| <u>Respond (RS)</u> | Incident Management | RS.MA |
| | Incident Analysis | RS.AN |
| | Incident Response Reporting and Communication | RS.CO |
| | Incident Mitigation | RS.MI |
| <u>Recover (RC)</u> | Incident Recovery Plan Execution | RC.RP |
| | Incident Recovery Communication | RC.CO |

NIST CSF 2.0 Resources

TRAVELING THROUGH NIST'S CYBERSECURITY FRAMEWORK (CSF) 2.0 RESOURCES

CSF 2.0

For industry, government, and organizations
to reduce cybersecurity risks



IMPLEMENTATION EXAMPLES

Review action-oriented steps to help you achieve
various outcomes of the subcategories



QUICK START GUIDES

For organizations with specific common goals



MAPPINGS

See how NIST's work interrelates and
shares themes



CSF 2.0 Resource Library

An official website of the United States government [Here's how you know](#)

NIST Search NIST

CYBERSECURITY FRAMEWORK

Helping organizations to better understand and improve their management of cybersecurity risk

CSF 2.0 Resource Center

- Download (PDF)
- Quick Start Guides
- Profiles
- Informative References
- FAQs
- Translations
- CSF 2.0 Tool

News and Events

Related Programs

Ways to Engage

Cybersecurity @ NIST

CSF 1.1 Archive

CONNECT WITH US

BIG NEWS | The NIST CSF 2.0 has been released, along with other supplementary resources!

CSF 2.0

For industry, government, and organizations to reduce cybersecurity risks

[Read the Document](#)

CSF 2.0 Profiles

Templates and useful resources for creating and using both CSF profiles

[See the Profiles](#)

Quick Start Guides

For users with specific common goals

[View the Quick Start Guides](#)

Informative References (Mappings)

See how NIST's resources overlap and share themes

[See the Mappings](#)

Suite of CSF 2.0 Resources

NIST Cybersecurity Framework 2.0: RESOURCE & OVERVIEW GUIDE

NIST Special Publication
NIST SP 1209
<https://doi.org/10.6028/NIST.SP.1209>
February 2024

NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide

NIST Special Publication
NIST SP 1209-1
February 2024

NIST Cybersecurity Framework 2.0: Quick-Start Guide for Creating and Using Organizational Profiles

NIST Special Publication
NIST SP 1209-2
February 2024

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](#)

NIST Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

Search CSRC | CSRC MENU

PROJECTS | CYBERSECURITY AND PRIVACY REFERENCE TOOL

Cybersecurity and Privacy Reference Tool CPRT

The NIST Cybersecurity Framework 2.0 Draft, Version 2.0

Search: [Search](#)

CPRT / Version 2.0

[Expand Entire Reference Dataset](#) [Export](#)

Functions

- GV GOVERN**
Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy
- ID IDENTIFY**
Help determine the current cybersecurity risk to the organization
- PR PROTECT**
Use safeguards to prevent or reduce cybersecurity risk
- DE DETECT**
Find and analyze possible cybersecurity attacks and compromises
- RS RESPOND**
Take action regarding a detected cybersecurity incident
- RC RECOVER**

NIST Cybersecurity Framework (CSF) 2.0 Reference Tool

Search:

Function
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy,

- Category**
Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)
- Subcategory**
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management (formerly ID.BE-02, ID.BE-03)
Implementation Examples
Ex1: Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission
- Subcategory**
GV.OC-02: Internal and external stakeholders are determined, and their needs and expectations regarding cybersecurity risk management are understood.

CYBERSECURITY FRAMEWORK

Informative References

CSF 2.0 Informative Reference Catalog

See what documents have been mapped to the CSF 2.0 Document.

[Catalog](#)

Compare CSF 2.0 Informative References

Generate Comparison Reports between CSF 2.0 Informative References you've selected.

[Comparison Reports](#)

Download Informative Reference in the Core

Directly download all the Informative References for CSF 2.0

[Download \(All\)](#) [Download \(Just\)](#)

CSF Resources for Healthcare

CPRT Mapping of HIPAA to CSF 1.1

| Category | Subcategory | Reference Items ⓘ |
|--|--|--|
| <p>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.</p> <p>✓ Hide all ID.AM References ⓘ</p> <ul style="list-style-type: none">+ 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 | <p>ID.AM-1: Physical devices and systems within the organization are inventoried</p> <p>✓ Hide all ID.AM-1 References ⓘ</p> <ul style="list-style-type: none">+ 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<ul style="list-style-type: none">• 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 | <p>CIS CSC: 1</p> <p>COBIT 5: BAI09.01, BAI09.02</p> <p>ISA 62443-2-1:2009: 4.2.3.4</p> <p>ISA 62443-3-3:2013: SR 7.8</p> <p>ISO/IEC 27001:2013: A.8.1.1, A.8.1.2</p> <p>NIST SP 800-53 Rev. 4: CM-8, PM-5</p> |

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

NIST Cybersecurity White Paper
NIST CSWP 32 ipd

NIST Cybersecurity Framework 2.0: A Guide to Creating Community Profiles

Initial Public Draft

Cherilyn Pascoe
*National Cybersecurity Center of Excellence
National Institute of Standards and Technology*

Julie Nethery Snyder
The MITRE Corporation

Karen Scarfone
Scarfone Cybersecurity

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.CSWP.32.ipd>

February 26, 2024

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)

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

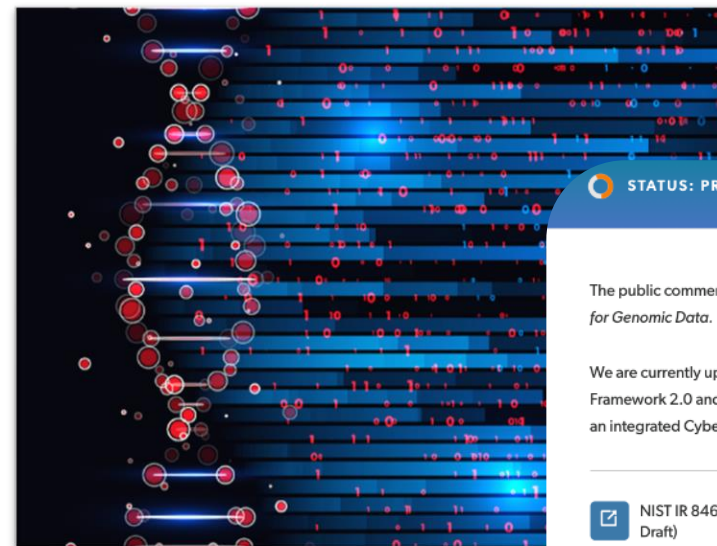
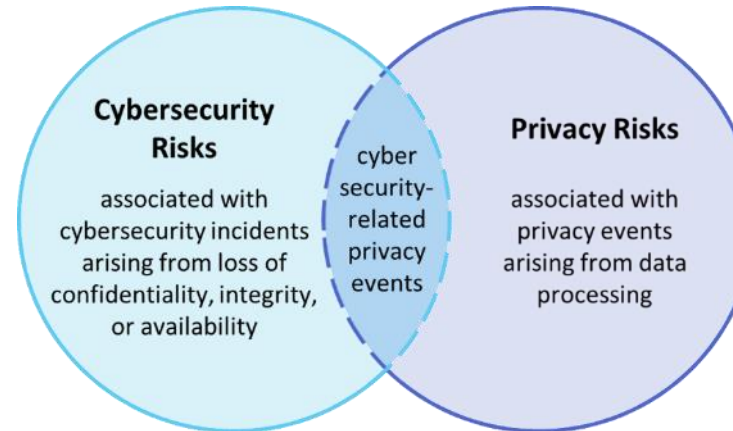
NIST SP 1800-1: Securing Electronic Health Records on Mobile Devices

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 | cpert@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 |

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

Who We Are

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



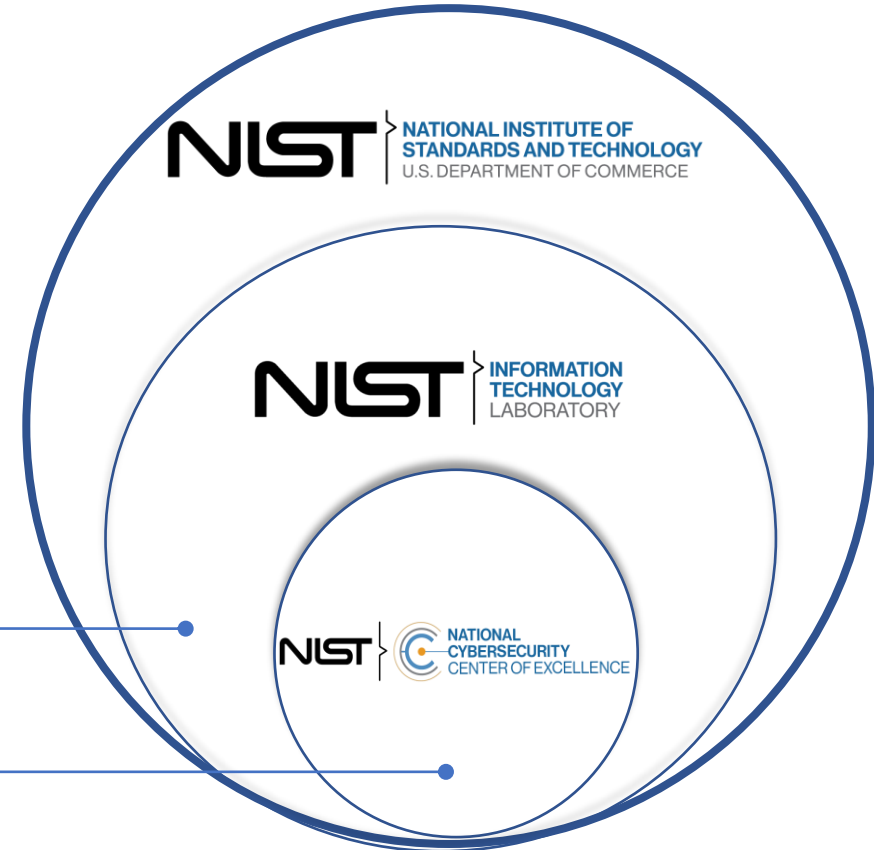
Who We Are

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**.

Information Technology Laboratory

Applied Cybersecurity Division



Guidance Created With Industry, For Industry



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

| By Technology | By Sector | By Community | By Status |
|------------------------------------|-------------------------------|---------------------------|-----------------------|
| 5G Cybersecurity | Consumer Data Protection | Framework Resource Center | Defining Scope |
| Applied Cryptography | Energy | | Seeking Collaborators |
| Artificial Intelligence | Financial Services | | Preparing Draft |
| Critical Cybersecurity Hygiene | Healthcare | | Soliciting Comments |
| Cybersecurity for the Space Domain | Manufacturing | | Reviewing Comments |
| Data Classification | Public Safety/First Responder | | Finalized Guidance |
| Data Security | Water/Wastewater | | Archived |
| DevSecOps | | | |
| Digital Identities - mDL | | | |
| Genomics Cybersecurity | | | |
| Internet of Things (IoT) | | | |
| IPv6 | | | |
| Mobile Device Security | | | |
| Supply Chain Assurance | | | |
| Trusted Cloud | | | |
| Zero Trust Architecture | | | |

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-jpg/>

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 (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



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



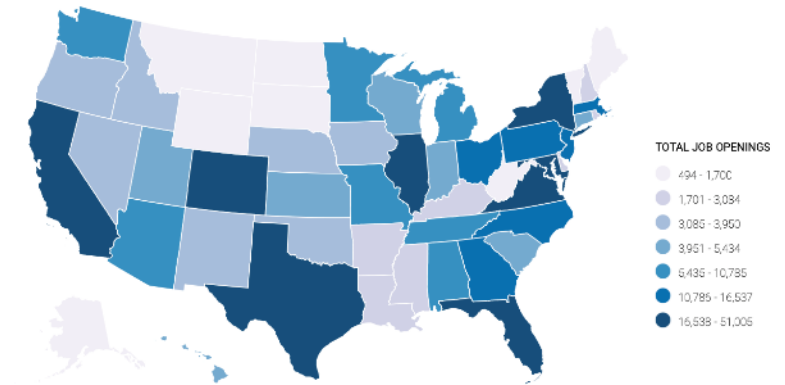
What is the Cybersecurity Workforce?

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)

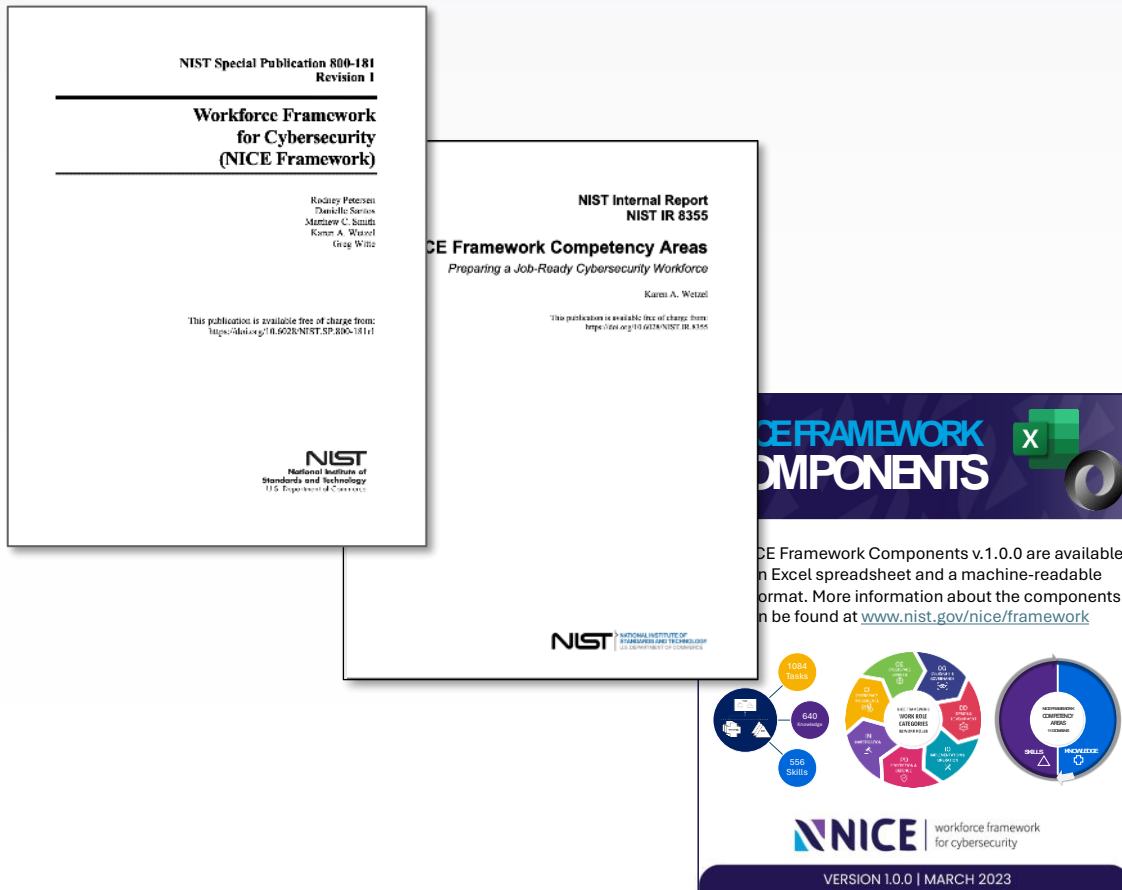


- Nearly 265,000 more cybersecurity workers needed to close current US supply gap
- Cybersecurity workforce has expanded each year since 2013
- Sep. 2023 – Aug. 2024: 457,398 cybersecurity job postings
- 1.25 million people currently work in cybersecurity roles
- Enough workers to fill only 83% of the 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 Framework)

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

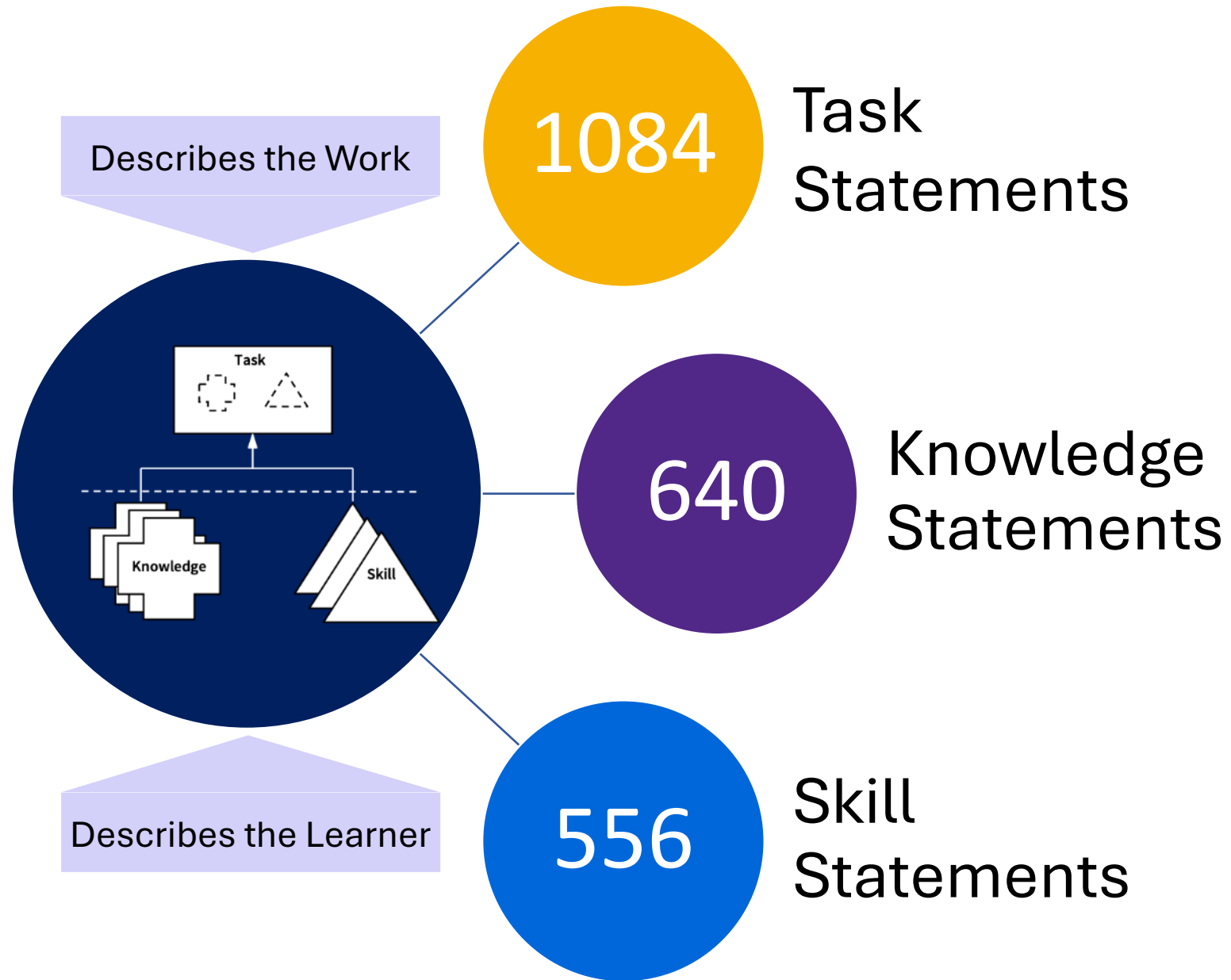


- ✓ A **common language** to clearly share about what a workforce needs to know
- ✓ A **modular, building-blocks approach** based on Task, Knowledge, and Skill (TKS) statements
- ✓ Defined **Work Roles** and **Competency Areas** for use in:
 - Career discovery
 - Education and training
 - Workforce planning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

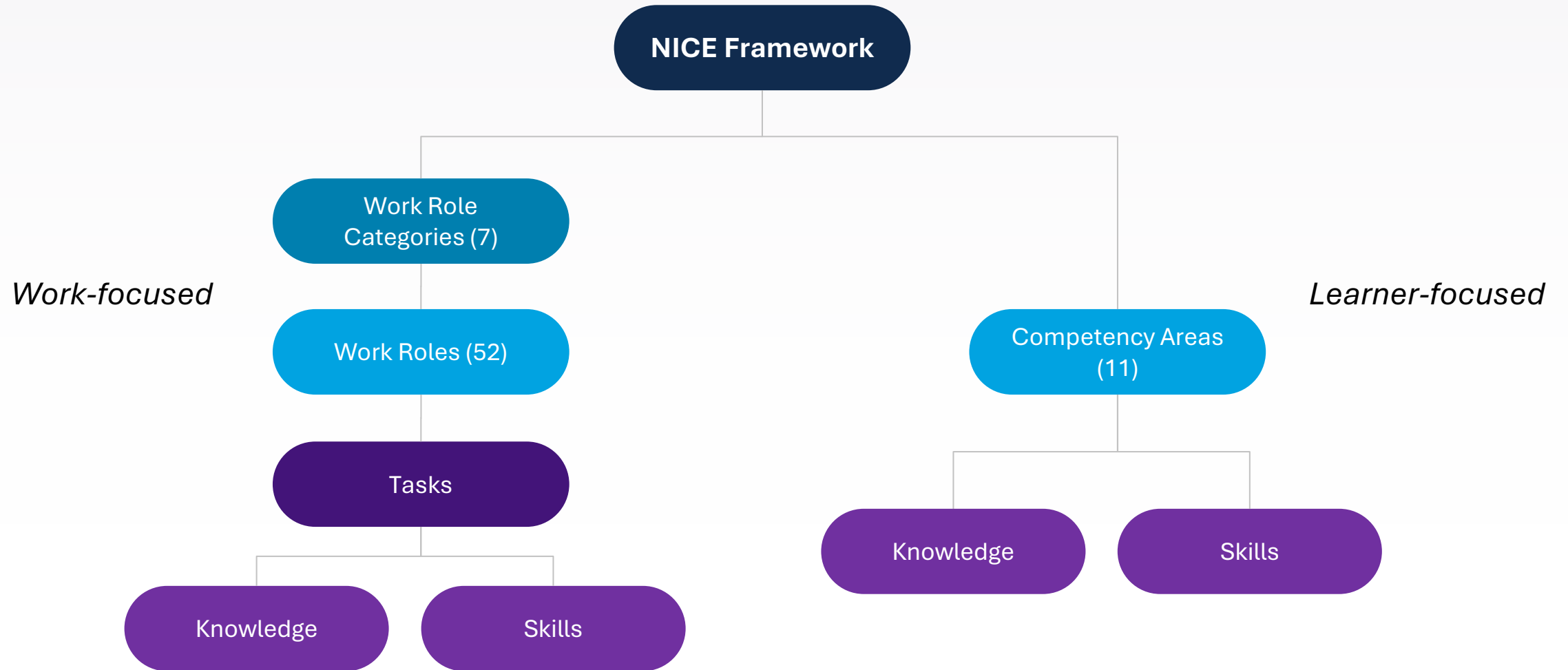
TKS Statements

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.



NICE Framework Structure



7 Work Role Categories

52 Work Roles



OVERSIGHT & GOVERNANCE



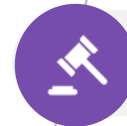
DESIGN & DEVELOPMENT



IMPLEMENTATION & OPERATION



PROTECTION & DEFENSE



INVESTIGATION



CYBERSPACE INTELLIGENCE



CYBERSPACE EFFECTS

Work Role Examples

| | |
|---|---|
| <p>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.</p> | <p>Work Role Category: Implementation and Operation (IO) Provides implementation, administration, configuration, operation, and maintenance to ensure effective and efficient technology system performance and security.</p> |
| <p>Vulnerability Analysis PD-WRL-007 OPM Code: 541</p> | <p>Database Administration IO-WRL-002 OPM Code: 421</p> |
| <p>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.</p> | <p>Responsible for administering databases and data management systems that allow for the secure storage, query, protection, and utilization of data.</p> |
| <ul style="list-style-type: none"> • 15 Task statements • 64 Knowledge Statements • 18 Skill statements | <ul style="list-style-type: none"> • 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 |

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.

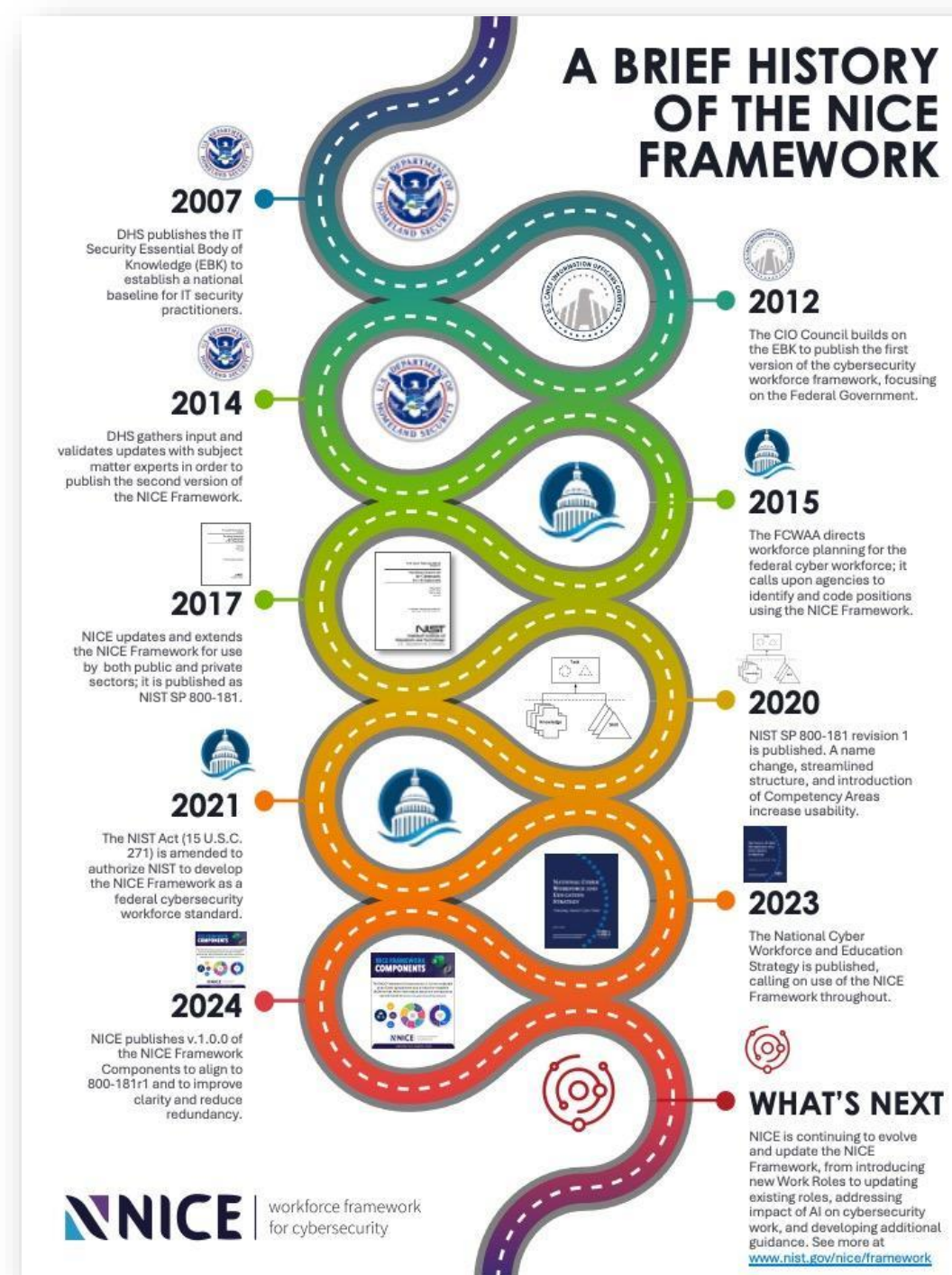
»» **Resource:** [NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce](#)

- 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

Development Process

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

»» Resource: [NICE Framework Revisions](#)



CALL FOR COMMENTS

Comments Requested on Proposed Updates for Three NICE Framework Work Roles and One NICE Framework Competency Area

[Learn More](#)

Comments due by: November 14, 2024, 11:59 p.m. ET.

www.nist.gov/nice/framework

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

| 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 |





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)

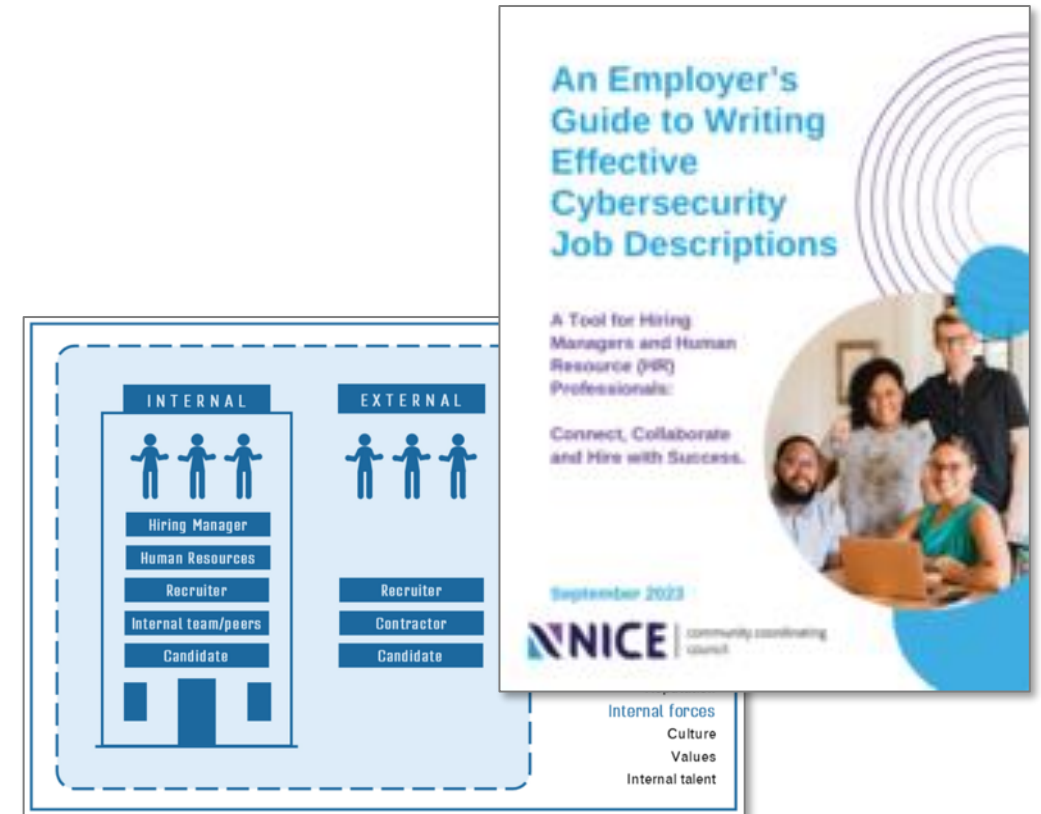
Three-step Approach:

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



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 | | |

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 abilities 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 Defense Forensics Analyst (IN-FOR-002).

<https://cybersecurity.usajobs.gov/job/756222600>

<https://www.usajobs.gov/job/746332400>



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



Example Use: Career Development

Career Pathways

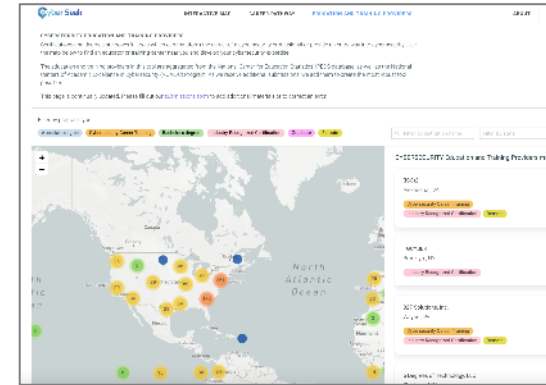
Upskilling & Reskilling

Demonstrating Capability



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](#)



Free and Low Cost Online Cybersecurity Learning Content

Today is the day to explore ways to improve your cybersecurity knowledge, skills, or even prepare for new career opportunities. If you are interested in cybersecurity careers, there are numerous online education providers to choose from. Many online courses are available from your local community college, four-year universities, even the prestigious [Centers of Academic Excellence](#) programs – please review all options.

The following links are for free and low-cost online educational content on topics such as information technology and cybersecurity. Some, not all, may contribute towards professional learning objectives or lead to industry certifications and online degrees. Please note that this site will continue to be updated as new information is gathered and edited for clarity and accuracy.

Career and Professional Development

Educator Training and Curriculum

Employee Awareness Training

K12 Education and Games

NICCS Cyber Career Pathway Tool

NICCS[®]
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

Education & Training Workforce Development Cybersecurity & Career Resources

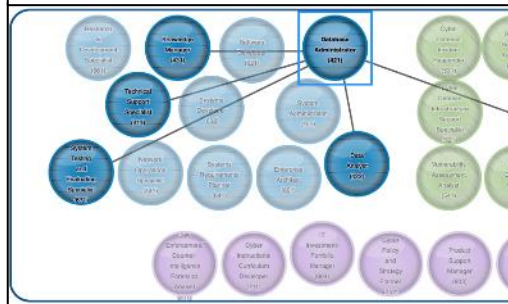
Workforce Development Cyber Career Pathways Tool

Cyber Career Pathways Tool

[User Guide](#)

This tool presents a new and interactive way to explore work roles within the Workforce Framework for Cybersecurity (NICE Framework). It depicts the Cyber Workforce according to five distinct, yet complementary, skill communities. It also highlights core attributes among each of the 52 work roles and offers actionable insights for employers, professionals, and those considering a career in Cyber. To start, select a work role below, or enter keywords in the search bar.

As a new feature within Cyber Career Pathways Tool, the micro-challenges ([TryCyber](#)) consist of hands-on experiences that allow users to complete several core cybersecurity workforce tasks. The following cybersecurity workforce roles have available challenges: [Technical Support Specialist](#), [System Administrator](#), [Network Operations Specialist](#), [Systems Security Analyst](#), [Database Administrator](#), [Data Analyst](#), [Cyber Defense Analyst](#), [Cyber Defense Incident Responder](#), [Vulnerability Assessment Analyst](#), and [Law Enforcement/Counterintelligence Forensics Analyst](#).



TRY CYBER [BETA]

SELECT CHALLENGE

| | |
|--|---|
| Network Operations Specialist Difficulty: ☆ Mentor: Aid Colt in adding additional IP addresses to a server's network interface. | Systems Administrator Difficulty: ☆ Mentor: Assist Skyla in managing system privileges by adding users to privileged groups. |
| Technical Support Specialist Difficulty: ☆ Mentor: Assist Tomás in provisioning new user accounts on a system for new employees. | Cyber Defense Incident Responder Difficulty: ☆ ☆ Mentor: Help Sofia collect intrusion artifacts from packet captures containing evidence of a cyber-attack. |

Career Pathway Roadmap

Welcome to the Cyber Career Roadmap (Multi-Pathway Tool)!

This digital tool offers an interactive way for working professionals (cyber and non-cyber), employers, students, and recent grads to explore and build their own career roadmap across the 52 different NICE Framework work roles. The start of your next cyber journey is only a few clicks away.

Users can select up to five work roles to learn more about their shared skillsets, alignment to the Cyber Skill Communities, or related specialization and functions. The Cyber Career Roadmap highlights the mobility between these connection points to help you and others determine the next steps in your career progression and skillset development. The tool also offers recommended on/off-ramps (i.e. steppingstones) and secondary work roles to consider and pursue in your career roadmap.

No matter where you are in your cyber career, the Cyber Career Roadmap provides a starting point in career planning.

To get started, select from three to five work roles of interest, or use the search bar.

Data Analyst [X]

↓ 5.04% KSAT overlap

Cyber Defense Analyst [X]

Select a third Work Role [v]

Begin typing to search work role names.

Communities

- IT
- Cybersecurity
- Cyber Effects
- Intel (Cyber)
- Cross Functional

[Clear all selections](#)

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

<https://trycyber.us/>

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 ⓘ

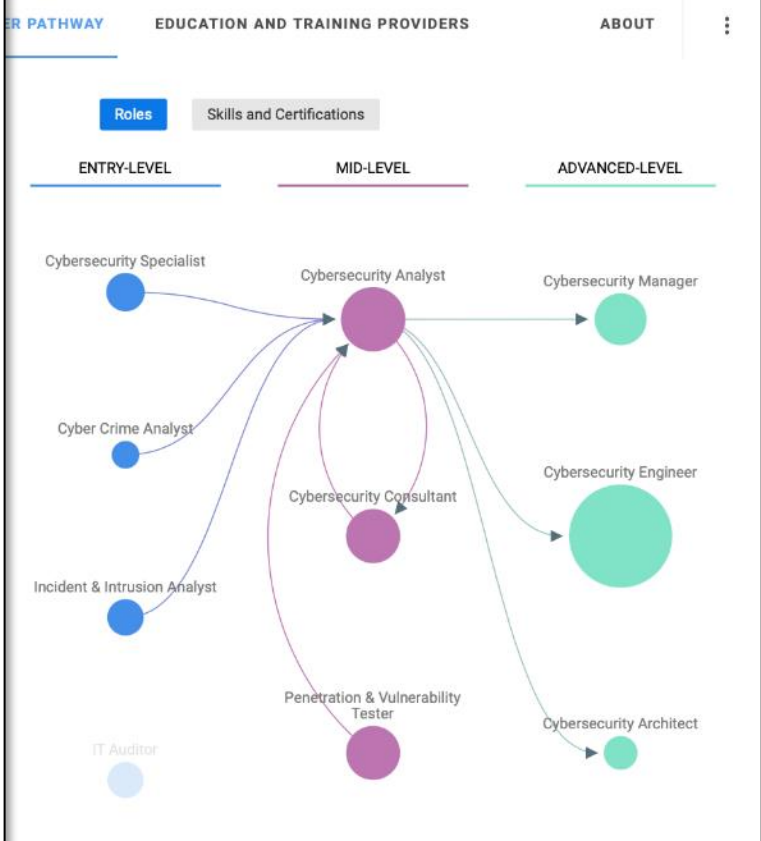
- Securely Provision
- Operate and Maintain
- Protect and Defend
- Analyze
- Investigate
- Oversee and Govern
- Collect and Operate

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)



SFIA Mapping to NICE Work Roles

The global skills and competency framework for the digital world

Home / Help and resources / SFIA - a framework for cyber security skills

SFIA - a framework for cyber security skills

... building security skills into every professional job for a security-minded culture ...

Using SFIA for cyber security

SFIA can be used in any workforce management activity. In cybersecurity talent management, a skills-based approach to recruitment, targeted professional development, real-world skills and responsibilities; so that employees are workforce agile and prepared for emerging threats. The mapping of cybersecurity skills and responsibilities across multiple roles in the organization, not just within specialist positions.

[SFIA and skills management](#)

Click image to expand.

- Skills-based recognition
- Certification
- Job levelling

- Cybersecurity operating model
- Cybersecurity job and role design
- Forecast cybersecurity skills needs

- Up-skilling & re-skilling
- Cyber education and training
- Cyber career pathways
- 70:20:10 / continuous learning

- Targeted talent acquisition
- Skills-based hiring

- Skills gap analysis
- Adjacent and transferable skills

- Skills-based assignments
- Flexible/dynamic role definition

- Skills inventory
- Potential for re-skilling

The 7 levels describe increasing responsibility, accountability and impact

| | 1 Follow | 2 Assist | 3 Apply | 4 Execute | 5 Plan, advise | 6 Initiate, influence | 7 Set strategy, create, maintain |
|--|----------|----------|---------|-----------|----------------|-----------------------|----------------------------------|
| 1 Follow Performs routine tasks under close supervision, follows instructions, and requires guidance to complete their work. | | | | | | | |
| 2 Assist Provides assistance to others, works under routine supervision, and uses their discretion to address routine problems. | | | | | | | |
| 3 Apply Performs varied tasks, sometimes complex and non-routine, using standard methods and procedures. Works under general direction, exercises discretion, and manages their work within deadlines. | | | | | | | |
| 4 Execute Performs diverse complex activities, supports and supervises others, works autonomously under general direction, and contributes expertise to deliver team objectives. | | | | | | | |
| 5 Plan, advise Provides authoritative guidance in their field and works under broad direction, accountable for achieving workgroup objectives and managing work from analysis to execution and evaluation. | | | | | | | |
| 6 Initiate, influence Has significant organisational influence, makes high-level decisions, shapes policies, demonstrates leadership, fosters organisational collaboration, and accepts accountability in key areas. | | | | | | | |
| 7 Set strategy, create, maintain Operates at the highest organisational level, determines overall organisational vision and strategy, and assumes accountability for overall systems. | | | | | | | |

An organisation selects the applicable roles and levels based on their own organisation design and context. Below are some examples from NICE.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Executive Cyber Leadership | | | | | | | 7 |
| IS Security Manager | | | | | 5 | 6 | |
| Security control assessor | | | 3 | 4 | 5 | | |
| Software developer | | 2 | 3 | 4 | 5 | | |
| Secure software assessor | | | 3 | 4 | 5 | | |
| Security architect | | | | 4 | 5 | 6 | |
| System Administrator | 1 | 2 | 3 | 4 | | | |
| Cyber Defence Incident Responder | | 2 | 3 | 4 | 5 | | |
| Cyber Intel Planner | | | | | 5 | 6 | |
| Database Administrator | | 2 | 3 | 4 | 5 | | |
| Vulnerability Assessment Analyst | | 2 | 3 | 4 | 5 | | |
| Cyber Defence Infrastructure Support Specialist | 1 | 2 | 3 | 4 | 5 | | |

Organisations can have roles at different levels to facilitate skill development and career progression, and to align with the increasing complexity of tasks, decision-making authority, and responsibility at each level.

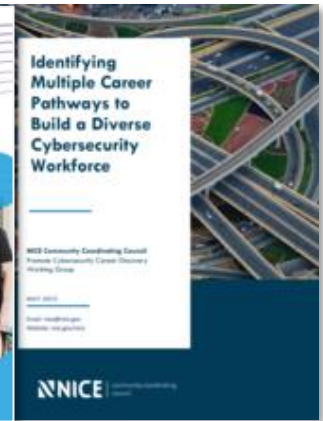
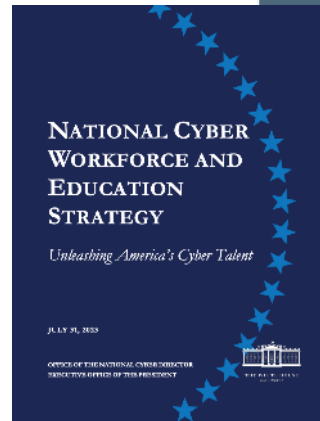
<https://sfia-online.org/en/tools-and-resources/sfia-views/sfia-view-information-cyber-security/mapping-nice-work-roles-to-sfia-skills>

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



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**



**U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights**

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

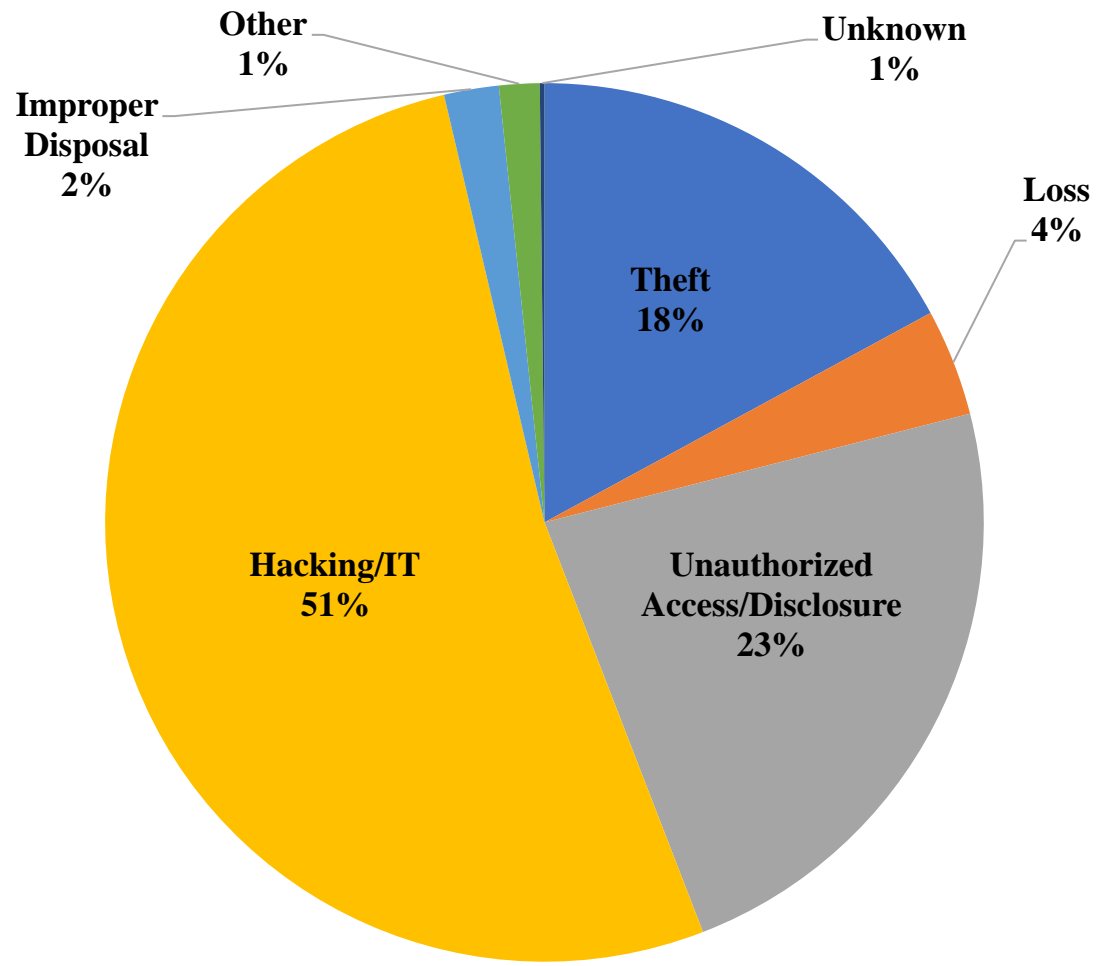
BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY



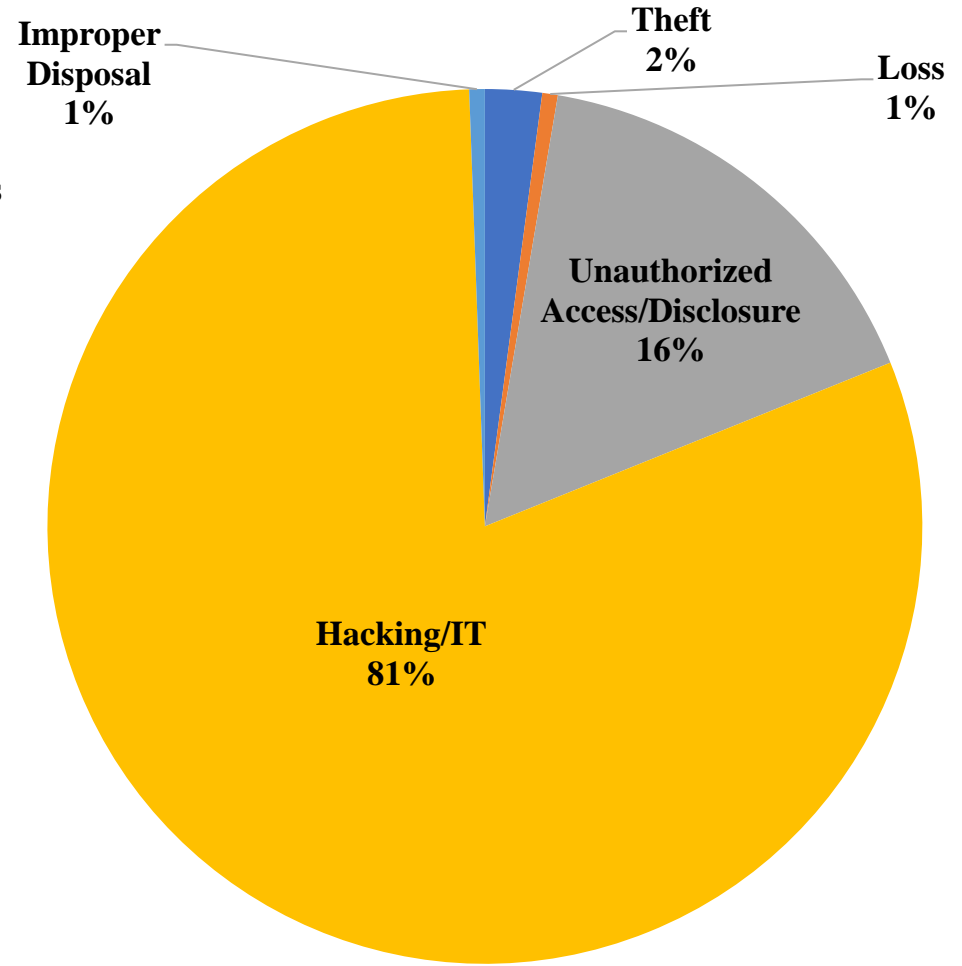
What Happens When OCR Receives a Breach Report

- 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



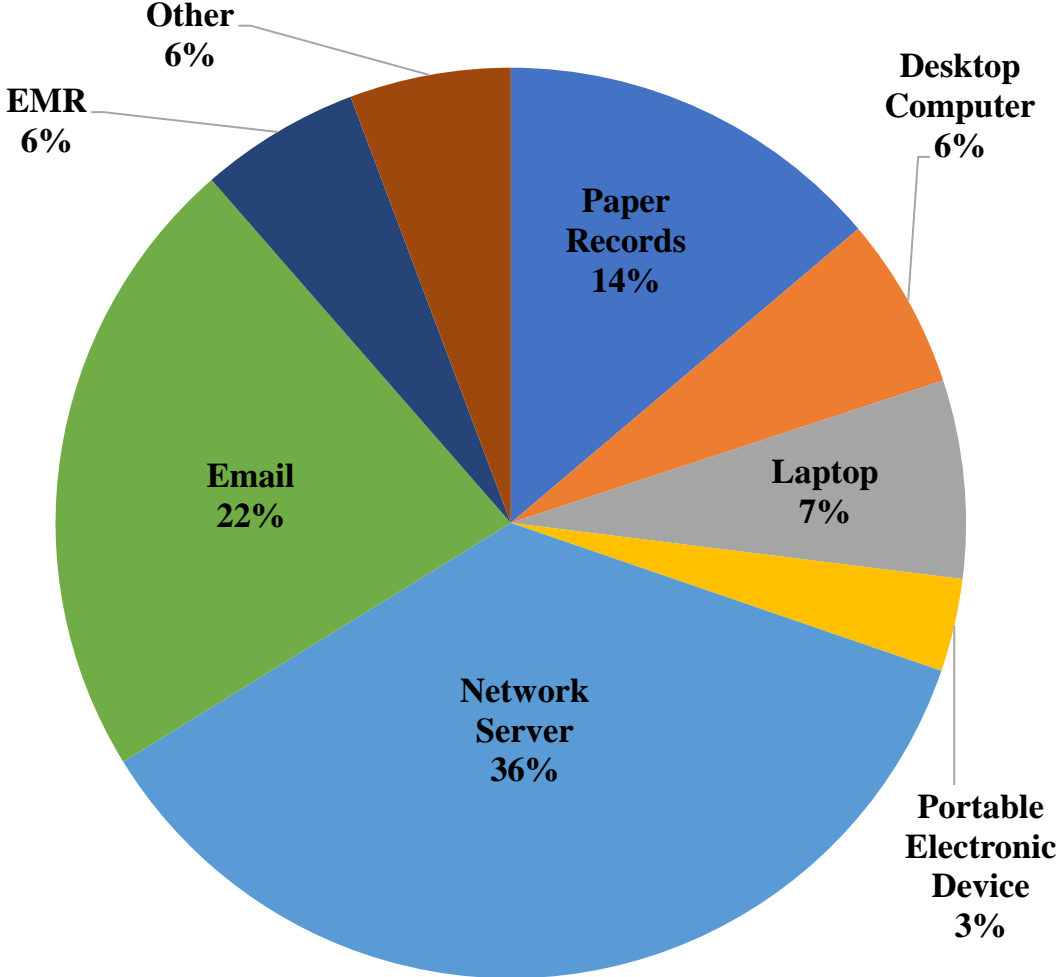
September 23, 2009 through Dec 31, 2023



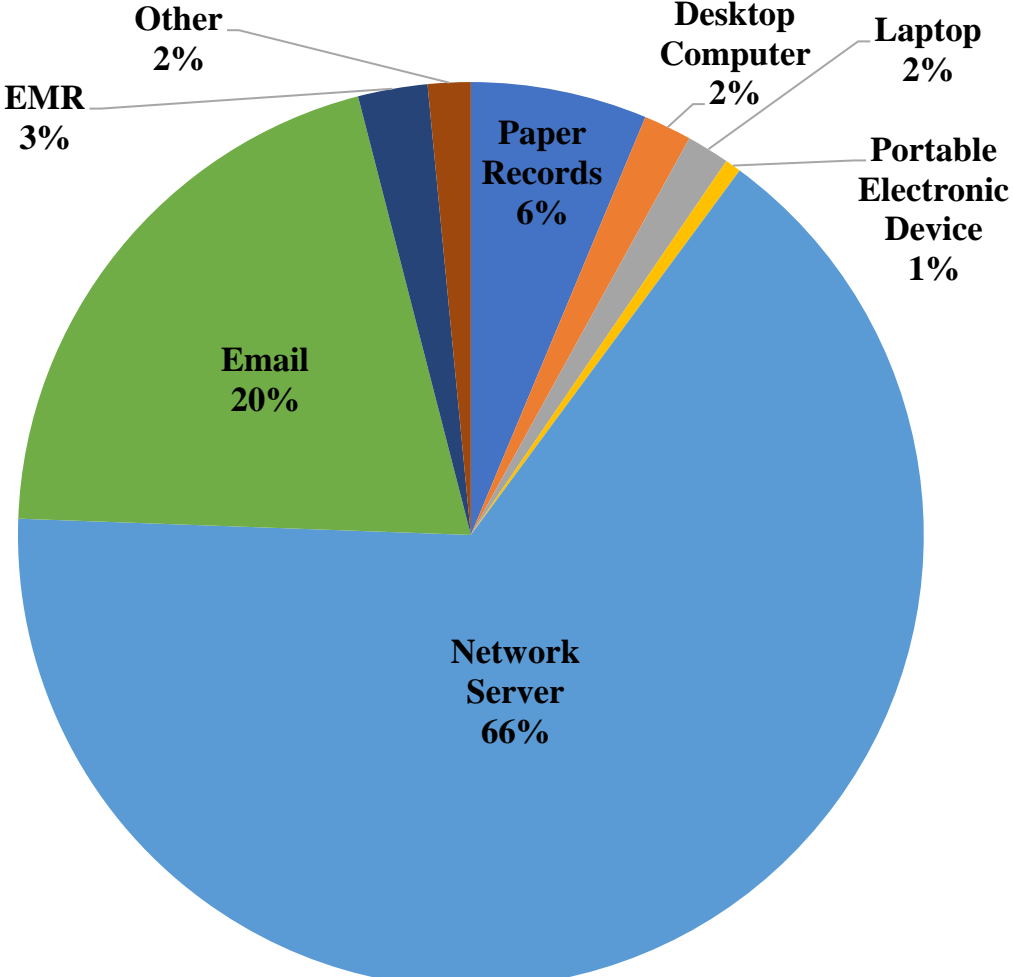
January 1, 2024 through September 30, 2024



500+ Breaches by Location of Breach



September 23, 2009 through Dec 31, 2023

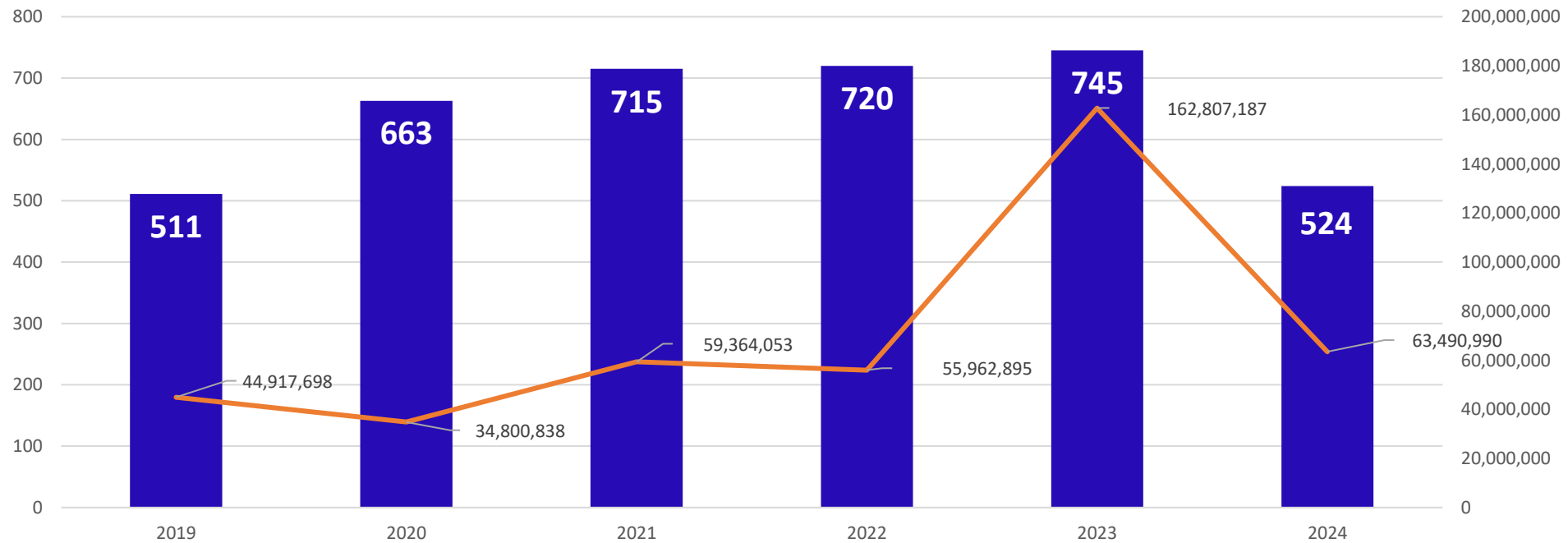


January 1, 2024 through September 30, 2024

Breaches Affecting 500 or More Individuals

Reports Received and Individuals Affected

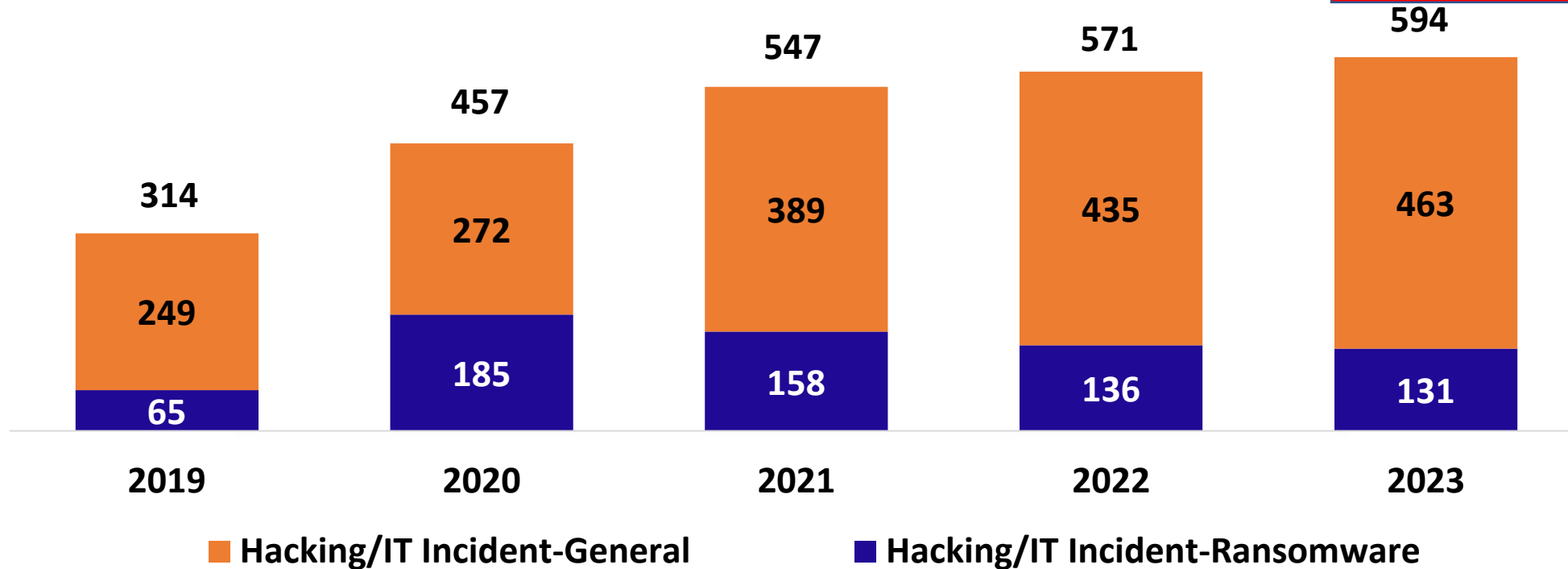
Calendar Years 2019 – August 2024



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

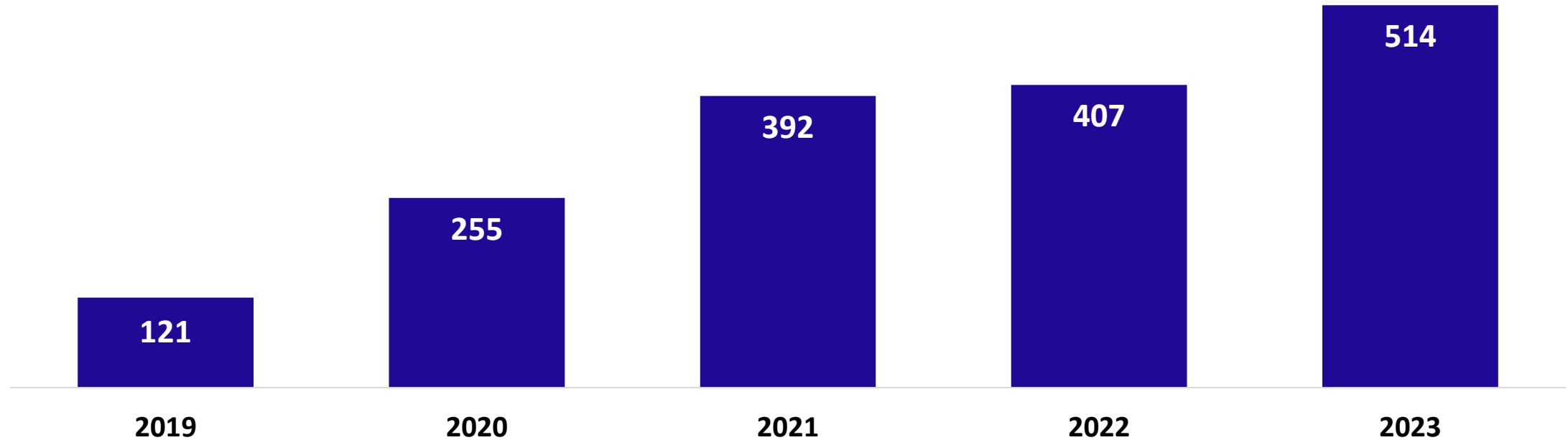
Calendar Years 2019 - 2023

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



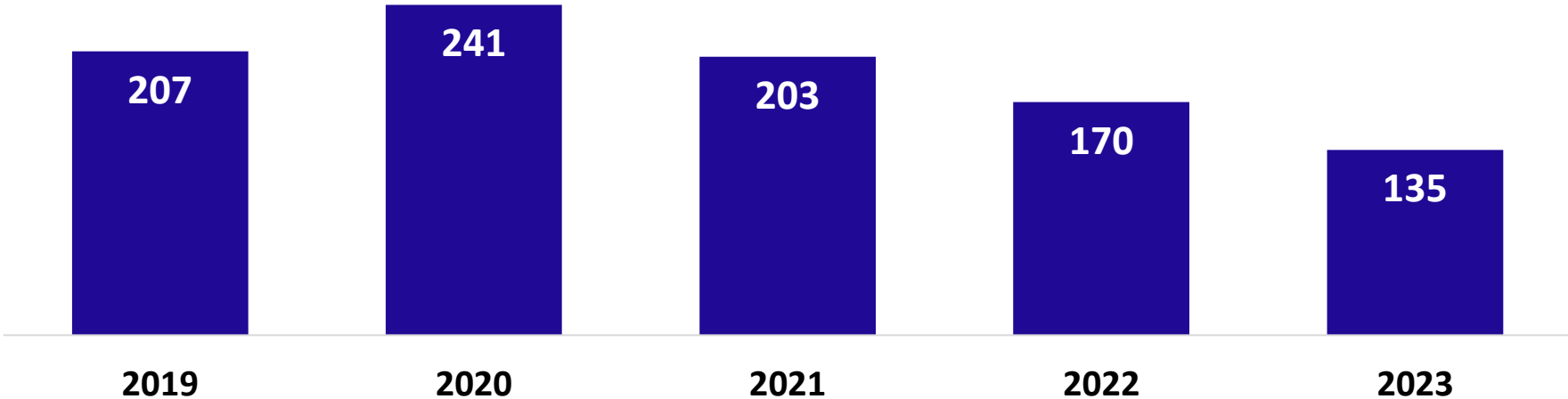
Breaches Affecting 500 or More Individuals Reports Received of Breaches Involving Network Servers

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 Virginia 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

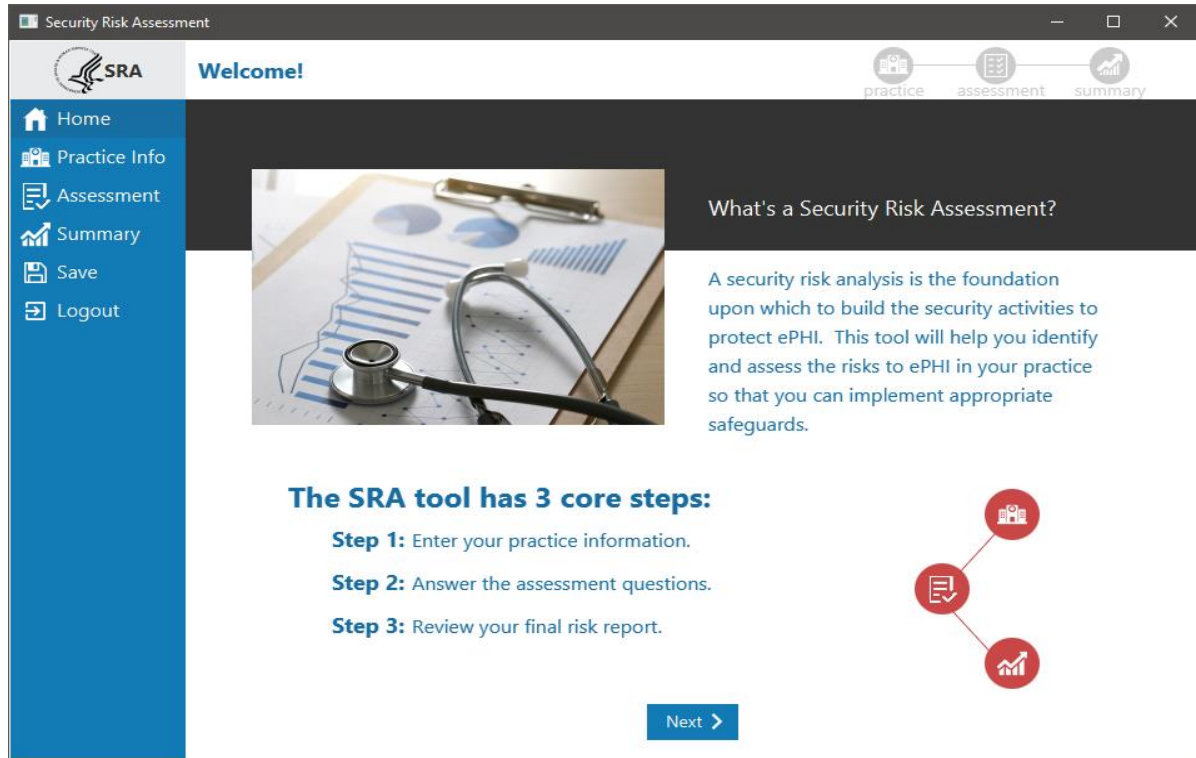
- New Enforcement Initiative
- Focus on compliance with key HIPAA Security Rule requirement
- Most OCR large breach investigations reveal a lack of a compliant risk analysis
- Drive better practices to protect electronic protected health information (ePHI)
- Better overall security of data

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



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office for Civil Rights