SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**

M8 Frameworks that describe the competencies

Contents

8.2 Frameworks that describe the competencies

- Cyber Career Pathways Tool. National Initiative for Cybersecurity Careers and Studies (cisa.gov)
- Department of Defense (DoD) Directive 8140/8570
- Enisa Skills Framework
- Framework and labor market

Nist Work Roles and Cyber Career Pathways Tool

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (CISA.GOV)

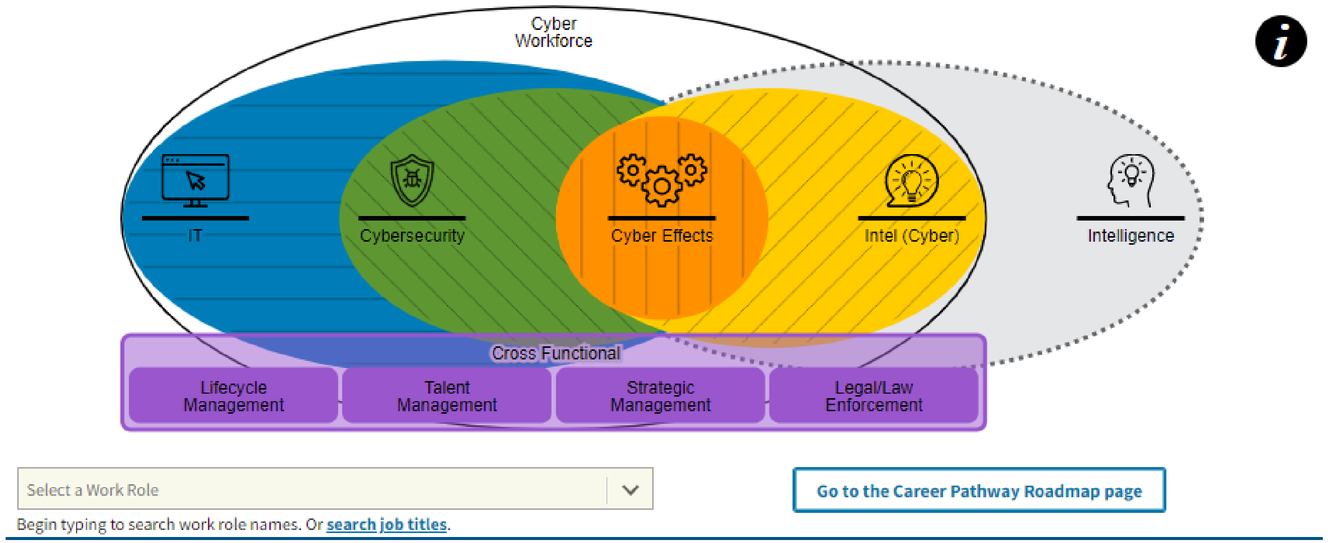
Nice framework defines 52 roles. They are divided in categories and specialty area.

Cyber Career Pathways Tool

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (CISA.GOV)

This online **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.

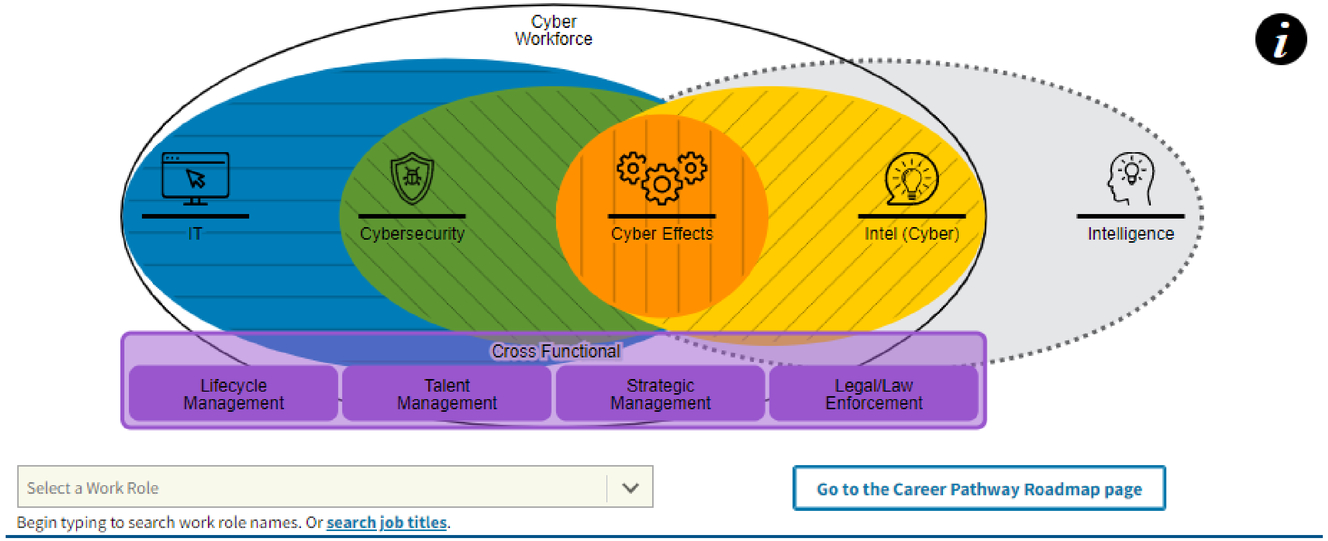
[Source: niccs.cisa.gov]



Cyber Career Pathways Tool

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (CISA.GOV)

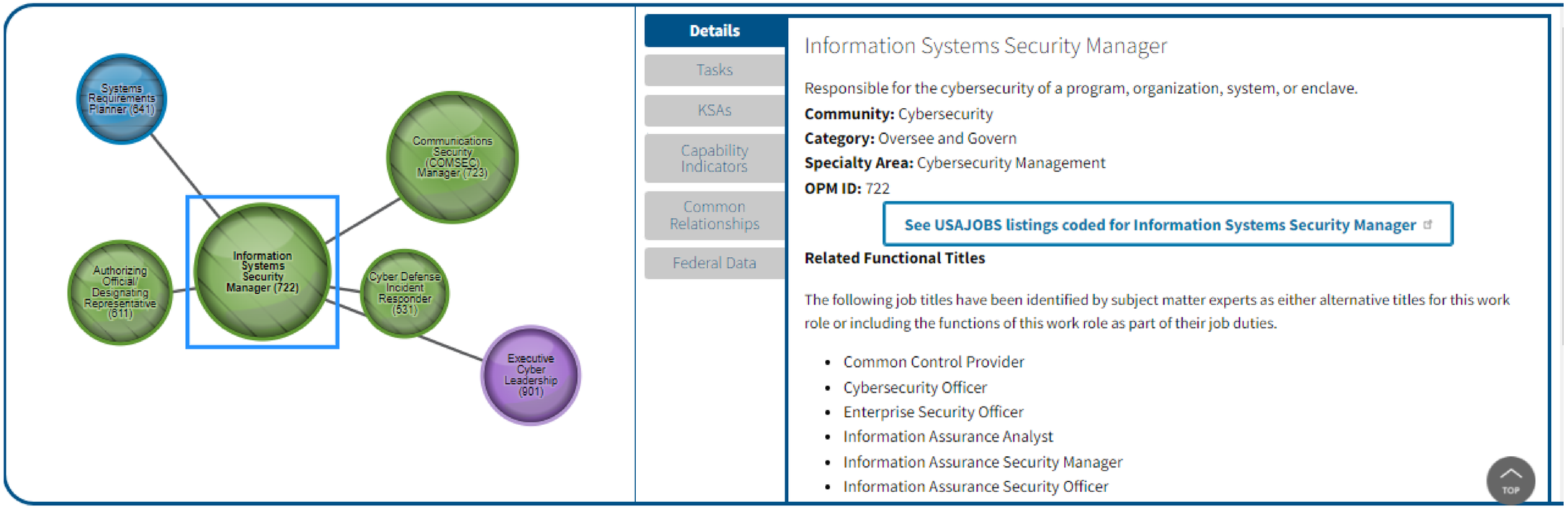
Users can select up to **five** work roles to learn more about their shared **skillsets**, alignment to the Cyber Skill **Communities**, or related *specialization* and *functions*. The Cyber Career Roadmap highlights the mobility between these connection points to help you and others determine the next 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*.



Cyber Career Pathways Tool

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (CISA.GOV)

Work Role: Information Systems Security Manager

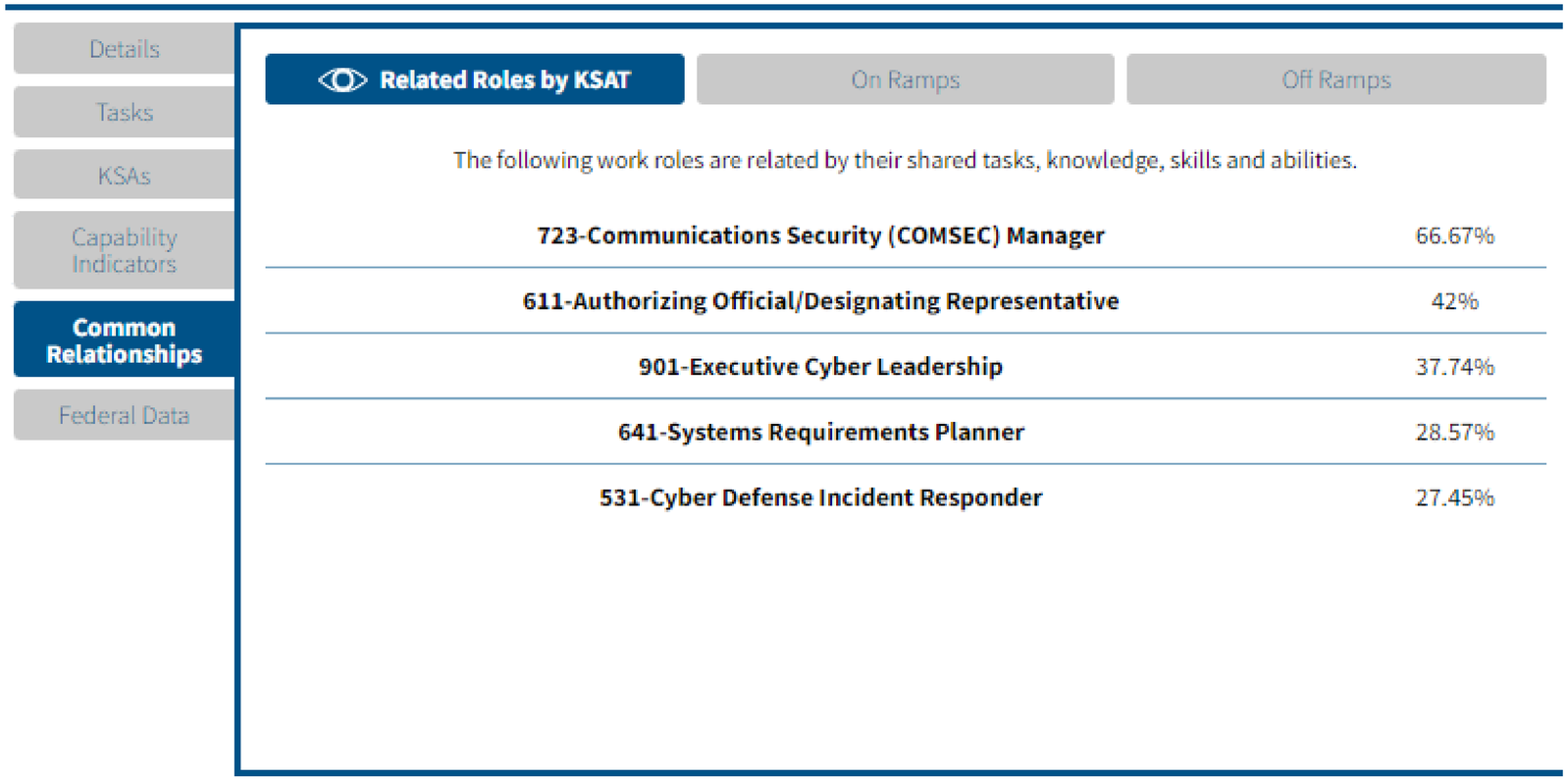


(the image above and following are example screenshots: they can't show all the information provided in the interactive tool)

Cyber Career Pathways Tool

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (CISA.GOV)

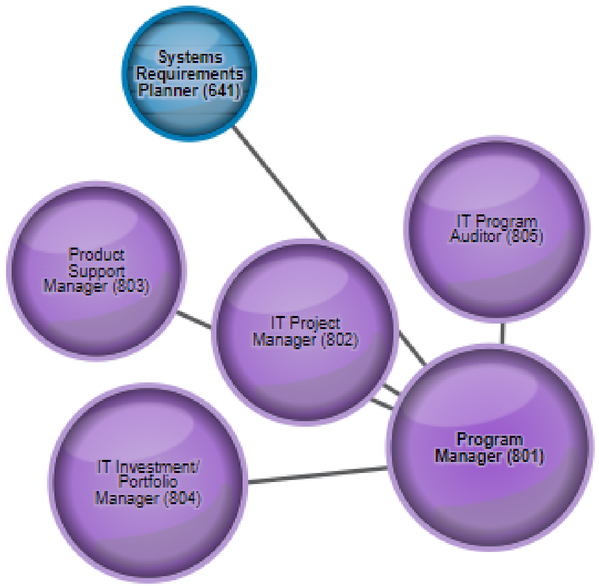
Work role: Information Systems Security Manager



Cyber Career Pathways Tool

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (CISA.GOV)

Work Role: Program Manager



Details

Tasks

KSAs

Capability Indicators

Common Relationships

Federal Data

Program Manager

Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.

Community: Cross Functional

Category: Oversee and Govern

Specialty Area: Program/Project Management and Acquisition

OPM ID: 801

See USAJOBS listings coded for Program Manager

Related Functional Titles

The following job titles have been identified by subject matter experts as either alternative titles for this work role or including the functions of this work role as part of their job duties.

- Compliance Manager
- Cybersecurity Officer
- Enterprise Security Officer
- Facility Security Officer
- IT / Cybersecurity Program Manager

Cyber Career Pathways Tool

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (CISA.GOV)

Work Role: Program Manager

	Entry	Intermediate	Advanced
Credentials/Certifications	**Recommended:** Not essential but may be beneficial **Example Types:** N/A **Example Topics:** Certifications that address requirements development and management processing, systems engineering, testing and evaluation, lifecycle logistics, contracting, business, cost, financial management, leadership, strategic program management, program lifecycle (initiating, planning, executing, controlling, closing), benefits management, stakeholder management, governance, and a data-driven approach and methodology for eliminating defects	**Recommended:** Yes **Example Types:** N/A **Example Topics:** Certifications that address project management (initiating, planning executing, monitoring and controlling, and closing), requirements development and management processing, systems engineering, testing and evaluation, lifecycle logistics, contracting, business, cost, financial management, leadership, strategic program management, program lifecycle (initiating, planning, executing, controlling, closing), benefits management, stakeholder management, governance, system security, network infrastructure, access control, cryptography, assessments and audits, and organizational security	**Recommended:** Yes **Example Topics:** Certifications that address strategic program management, program lifecycle (initiating, planning, executing, controlling, and closing), benefits management, stakeholder management, governance, security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, and software development security

Cyber Career Pathways Tool

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (CISA.GOV)

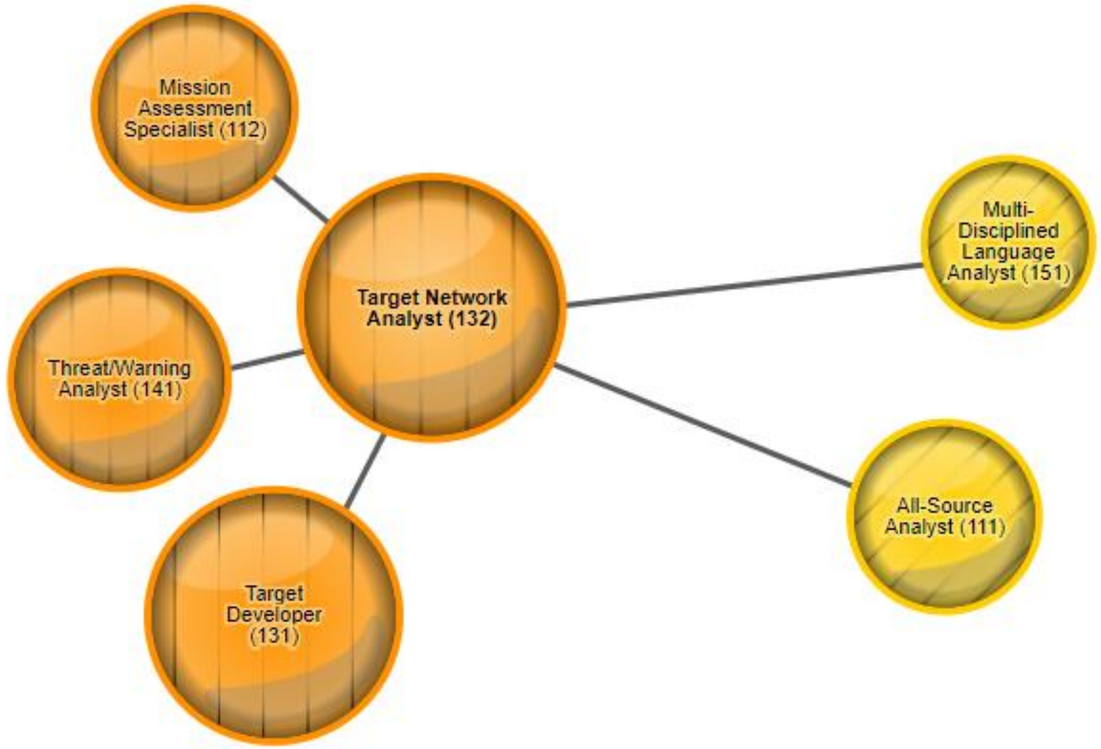
Work Role: Program Manager

Continuous Learning	**Recommended:** Yes **Examples:** 20-60 hours annually (may include maintaining certifications, attending symposium/ conferences, self-directed study, and taking higher education coursework)	**Recommended:** Yes **Examples:** 40-80 hours annually (may include conferences, maintaining certification, on-the-job training for next level/increasing responsibilities, developmental assignments, shadowing, rotations, seminars, conferences, brown bags, and presentations)	**Recommended:** Yes **Examples:** 40-120 hours annually (may include holding elected/ appointed positions [e.g., committee leadership roles or attending and/or presenting at educational conferences or meetings], mentoring, and maintaining certifications)
Education	**Recommended:** Not essential but may be beneficial **Example Types:** Associate's, Bachelor's **Example Topics:** Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	**Recommended:** Yes **Example Types:** Associate's, Bachelor's (certifications addressing advanced systems management, systems administration, information systems security, system certification, risk analysis, governance, security risk management, controls, audit management, information security core concepts [access control, social engineering, phishing attacks, and identity theft], strategic planning, finance, and vendor management may substitute for education) **Example Topics:** Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	**Recommended:** Yes **Example Types:** Master's, Ph.D. (certifications addressing advanced systems management, systems administration, information systems security, system certification, risk analysis, governance, security risk management, controls, and audit management, information security core concepts [access control, social engineering, phishing attacks, and identity theft], strategic planning, finance, and vendor management may substitute for education) **Example Topics:** Computer science, cybersecurity, information technology, software engineering, information systems, computer

Cyber Career Pathways Tool

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (CISA.GOV)

Position: Target Network Analyst



Target Network Analyst

Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.

Community: Cyber Effects

Category: Analyze

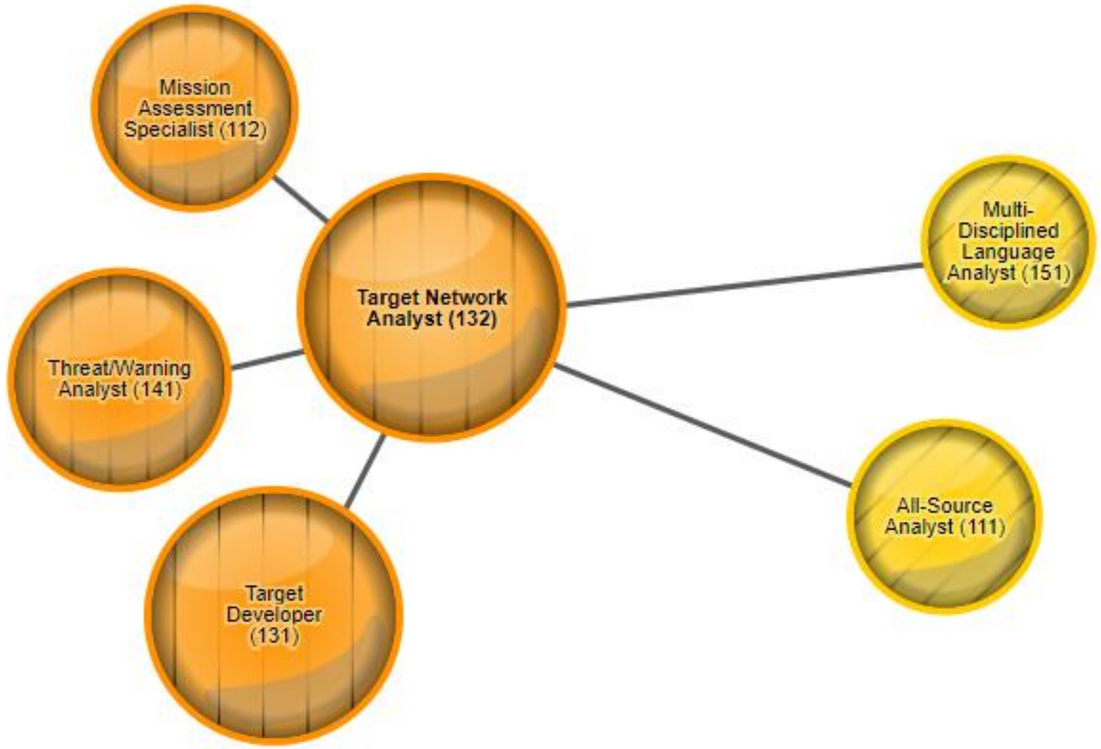
Specialty Area: Targets

OPM ID: 132

Cyber Career Pathways Tool

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (CISA.GOV)

Position: Target Network Analyst



Legend

C - Core Tasks

A - Additional Tasks

A* - Not included in the initial analysis to determine whether it is Core or Additional to the work role.

A	**T0582**	Provide expertise to course of action development.
C	**T0595**	Classify documents in accordance with classification guidelines.
C	**T0599**	Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.
C	**T0606**	Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.
A	**T0607**	Identify and conduct analysis of target communications to identify information essential to support operations.
C	**T0617**	Conduct nodal analysis.
C	**T0621**	Conduct quality control to determine validity and relevance of information gathered about networks.

(image is an example: other details for this position are provided)

U.S. Department of Defense (DoD)

DOD DIRECTIVE 8140/8570

What is DoDD 8140?

DoD Directive 8140, signed August 2015, establishes a definition for the cyber workforce and outlines Component roles and responsibilities for the management of the DoD cyber workforce. This was a replacement of 8570.01-M whose guidance and procedures is still in effect until such a time it is replaced for the training, certification, and management of all government employees and contractors who conduct cybersecurity functions. The individuals who hold these work roles are required to carry an approved certification for their job classification.

[Source: www.sans.org]

U.S. Department of Defense (DoD)

DOD DIRECTIVE 8140/8570

Who is affected by 8140 (8570)?
Any full- or part-time military service member in the U.S., contractor, or local nationals with privileged access to a DoD information system performing information assurance (security) functions – regardless of job or occupational series

[Source: www.sans.org]

U.S. Department of Defense (DoD)

DOD DIRECTIVE 8140/8570

DoDD 8140 Requires:
All personnel performing Information Assurance Technical and Information Assurance Management functions must be certified.

All personnel performing CSSP and IASAE roles must be certified.

All IA jobs will be categorized as '*Technical*' or '*Management*' Level I, II, or III, and to be qualified for those jobs, you must be certified.

[Source: www.sans.org]

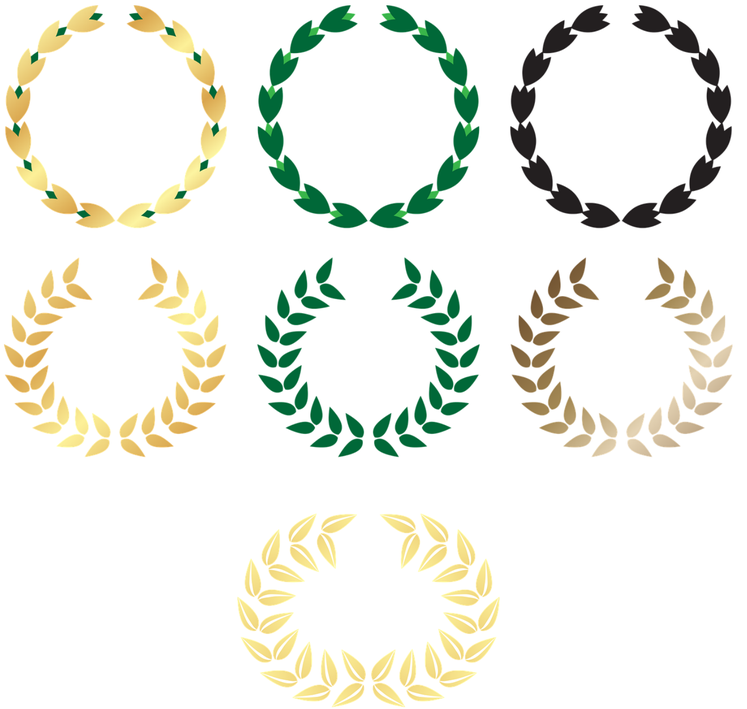
U.S. Department of Defense (DoD)

DOD DIRECTIVE 8140/8570

As an extension of the DoD 8570.01-Manual, some certifications have been approved as IA baseline certifications for the IA Workforce.

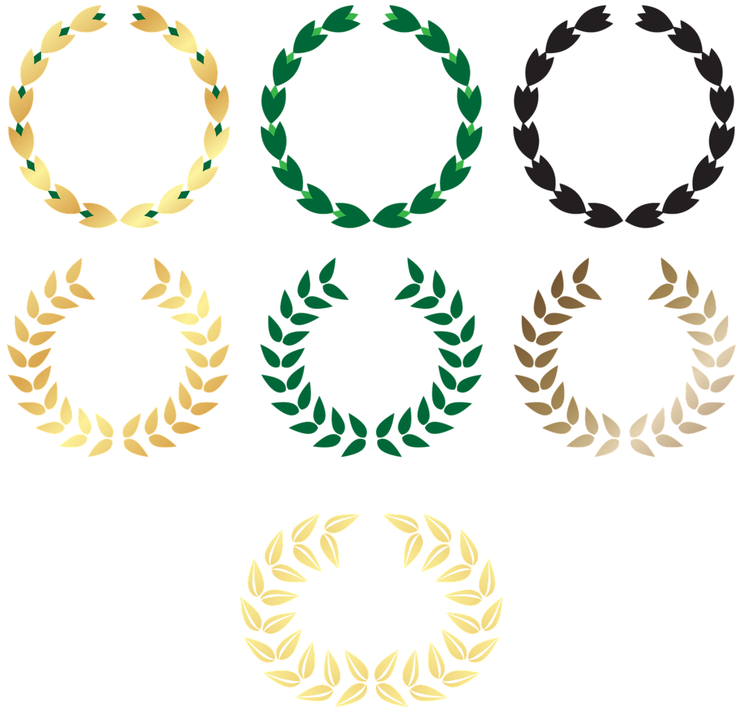
Personnel performing IA functions must obtain one of the certifications required for their position category or specialty and level. Refer to Appendix 3 of 8570.01-M for further implementation guidance.

https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/



Cyber Career Pathways
DoDD 8140/8570

Federal Cyber Career Pathways – DoD Cyber Exchange
This information was developed in partnership with the Interagency Federal Cyber Career Pathways **Working Group** (WG). The WG is dedicated to developing cyber career resources, including career pathways for NICE Framework work roles for use throughout the Federal Government, as well as private industry and academia.



Cyber Career Pathways
DoDD 8140/8570

The DoD Cyber Workforce Framework establishes the DoD's authoritative lexicon based on the **work** an individual is performing, not their position titles, occupational series, or designator.
The DCWF describes the work performed by the full spectrum of the cyber workforce as defined in DoD Directive (DoDD) 8140.01. The DCWF leverages the original National Initiative for Cybersecurity Education (*NICE*) Cybersecurity Workforce Framework (*NCWF*) and the DoD Joint Cyberspace Training and Certification Standards (*JCT&CS*).

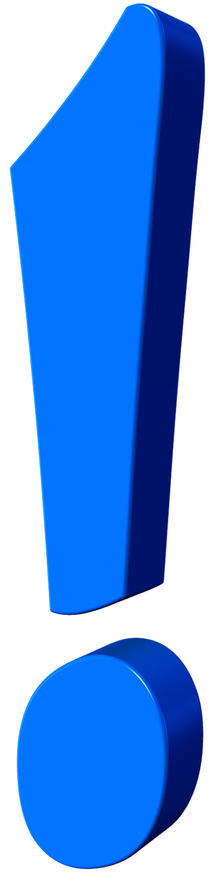
Nist-Nice Framework and DoDD 8140/8570

DIFFERENCES

Part of the confusion some have between these two frameworks is the entangled *origins* the two have. Firstly, the NICE Framework provides a baseline for federal cybersecurity but it is a *non-binding baseline*. In practice, the NICE Framework is used as a starting point for **federal agencies**.

Next, what makes this confusing is the fact that the DoD Cyber Workforce Framework (DCWF) was defined in both DoDD 8140 and the NICE Framework. To top off the confusion level, some jobs bleed into other jobs, which can ultimately cause security vulnerabilities.

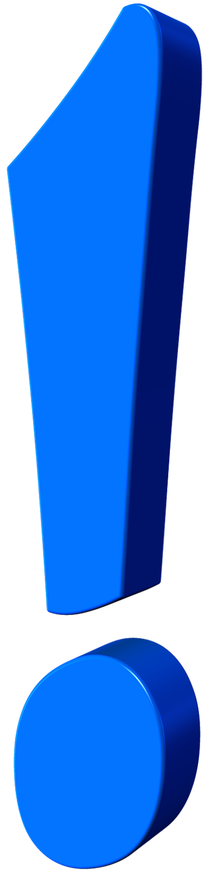
[Source: resources.infosecinstitute.com]



Nist-Nice Framework and DoDD 8140/8570

DIFFERENCES

The biggest difference between the NICE Framework and DoDD 8140 is their intended audience, or users and **stakeholders**. The NICE Framework is intended for a *broad range of federal government employees*, from the GSA to the FBI. DoDD 8140 is intended for *United States military users and stakeholders*. This may seem like a slight difference, but it has a huge impact on how these frameworks operate.



[Source: resources.infosecinstitute.com]

Nist-Nice Framework and DoDD 8140/8570

DIFFERENCES

The NICE Framework and DoDD 8140's differences are best viewed through the lens of the seven categories of the NICE Framework because of the different intended audiences. Let's take a look at how these framework's categories differ.

[Source: resources.infosecinstitute.com]

Nist-Nice Framework and DoDD 8140/8570

DIFFERENCES

- *Analysis*: NICE focuses on the acts of cybercriminals and 8140 focuses more on foreign intelligence agencies and foreign actors.
- *Collect & Operate*: 8140 focuses on counterintelligence and NICE has a counter-criminal focus.
- *Investigate*: NICE focuses on locking cybercriminals up and 8140 focuses on building developed and detailed target packages for future use.
- *Oversee & Govern*: 8140 places more emphasis on certification because it is more “baked in” for other federal agencies.
- *Securely Provision*: The biggest difference here is that 8140 has built out the Secret Internet Protocol Router Network, otherwise known as SIPRNet. While other federal agencies have secure networks, the heightened need for a secure network on the *battlefield* has given this category more **emphasis** for DoDD 8140.

[Source: resources.infosecinstitute.com]

Enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

The European Union Agency for Cybersecurity (**ENISA**) is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe.

ENISA contributes to EU *cyber policy*, enhances the *trustworthiness* of ICT products, services and processes with cybersecurity certification *schemes*, cooperates with Member States and EU bodies, and helps Europe prepare for the future *cyber challenges*.

[Source: enisa.europa.eu]

Enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

It states that the cybersecurity workforce **shortage** and **skills gap** is a major concern for both *economic development* and *national security*, especially in the rapid digitization of the global economy.

[Source: enisa.europa.eu]

Enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

It poses threats with a high impact on the data, information technology systems and networks that form the dorsal spine of **modern societies**.

This shortage can be *further analysed* into two concurrent issues: a **quantitative** one and a **qualitative** one. The quantitative issue is related to the insufficient supply of cybersecurity professionals to meet the requirements of the job market and the qualitative one is related to the inadequacy of professional skills to meet the market's needs.

[Source: enisa.europa.eu]

Enisa

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

The European Cybersecurity Skills Framework aims to create a *common understanding* of the **roles**, **competencies**, **skills** and **knowledge** used by and for individuals, employers and training providers across the EU Member States, in order to address the cybersecurity skills shortage.

[Source: enisa.europa.eu]

Enisa

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Additionally, it will help to further facilitate cybersecurity-related *skills recognition* and support the **design** of cybersecurity-related training programmes for *skills* and *career* development. Consequently, the European Cybersecurity Skills Framework will boost employment and employability in cybersecurity- related positions.

[Source: enisa.europa.eu]

Enisa

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Profile Title
Alternative Title(s) *Lists titles under the same profile*
Summary statement *Indicates the main purpose of the profile.*
Mission *Describes the rationale of the profile.*
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*

Profile Title
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*

Profile Title
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*
e-Competences (from e-CF)

[Source: European cybersecurity skills framework v. 0.5 draft, enisa.europa.eu]

Enisa

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

CISO:

2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)

Profile Title	Chief Information Security Officer (CISO)
Alternative Title(s) *Lists titles under the same profile*	Cybersecurity Programme Director Information Security Officer (ISO) Head of Information Security IT Security Officer
Summary statement *Indicates the main purpose of the profile.*	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.
Mission *Describes the rationale of the profile.*	Defines, maintains and communicates the cybersecurity vision, strategy, policies and procedures. Manages the implementation of the cybersecurity policy across the organisation. Assures information exchange with external authorities and professional bodies.
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity Strategy • Cybersecurity Policy

[Source: European cybersecurity skills framework v. 0.5 draft, enisa.europa.eu]

Enisa

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

CISO:

Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organisational objectives • Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution • Supervise the application and improvement of the Information Security Management System (ISMS) • Educate senior management about cybersecurity risks, threats and their impact to the organisation • Ensure the senior management approves the cybersecurity risks of the organisation • Develop cybersecurity plans • Develop relationships with cybersecurity-related authorities and communities • Report cybersecurity incidents, risks, findings to the senior management • Monitor advancement in cybersecurity • Secure resources to implement the cybersecurity strategy • Negotiate the cybersecurity budget with the senior management • Ensure the organisation's resiliency to cyber incidents • Manage continuous capacity building within the organisation • Review, plan and allocate appropriate cybersecurity resources
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Understand core organisational business processes • Assess and enhance an organisation's cybersecurity posture • Analyse and implement cybersecurity standards, frameworks, policies, regulations, legislations, certifications and best practices • Manage cybersecurity resources • Develop, champion and lead the execution of a cybersecurity strategy • Influence an organisation's cybersecurity culture • Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing • Review and enhance security documents, reports, SLAs and ensure the security objectives • Practice ethical cybersecurity organisation requirements

[Source: European cybersecurity skills framework v. 0.5 draft, enisa.europa.eu]

Enisa

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

CISO:

	• Provide practical solutions to cybersecurity issues • Establish a cybersecurity plan • Communicate, coordinate and cooperate with internal and external stakeholders • Apply relevant standards, best practices and legal requirements for information security • Anticipate required changes to the organisation's information security strategy and formulate new plans • Define and apply maturity models for cybersecurity management • Anticipate future cybersecurity threats, trends, needs and challenges in the organisation • Ability to lead multidisciplinary cybersecurity teams	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Knowledge of cybersecurity and privacy standards, frameworks, policies, regulations, legislations, certifications and best practices • Understanding of ethical cybersecurity organisation requirements • Knowledge of security controls • Knowledge of cybersecurity maturity models • Knowledge of cybersecurity tactics, techniques and procedures • Knowledge of resource management • Knowledge of management practices • Knowledge of risk management frameworks	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	D.1. Information Security Strategy Development E.3. Risk Management E.4. Relationship Management E.8. Information Security Management E.9. IS-Governance	Level 5 Level 4 Level 3 Level 4 Level 4

[Source: European cybersecurity skills framework v. 0.5 draft, enisa.europa.eu]

Enisa

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Penetration tester

2.12 PENETRATION TESTER

Profile Title	Penetration Tester
Alternative Title(s) *Lists titles under the same profile*	Pentester Ethical Hacker Vulnerability Analyst Cybersecurity Tester Offensive Cybersecurity Expert Defensive Cybersecurity Expert Red Team Expert
Summary statement *Indicates the main purpose of the profile.*	Assess the effectiveness of security controls, reveals and utilise cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors.
Mission *Describes the rationale of the profile.*	Plans, designs, implements and executes penetration testing activities and attack scenarios to evaluate the effectiveness of deployed or planned security measures. Identifies vulnerabilities or failures on technical and organisational controls that affect the confidentiality, integrity and availability of ICT products (e.g. systems, hardware, software and services).
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Technical Cybersecurity Assessment
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Identify, analyse and assess technical and organisational cybersecurity vulnerabilities • Identify attack vectors, uncover and demonstrate exploitation of technical cybersecurity vulnerabilities • Test systems and operations compliance with regulatory standards • Select and develop appropriate penetration testing techniques • Organise test plans and procedures for penetration testing • Establish procedures for penetration testing result analysis and reporting • Document and report penetration testing results to stakeholders • Deploy penetration testing tools and test programs

[Source: European cybersecurity skills framework v. 0.5 draft, enisa.europa.eu]

Enisa

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Penetration tester:

Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Develop codes, scripts and programmes • Perform social engineering • Identify and exploit vulnerabilities • Conduct ethical hacking • Think creatively and outside the box • Solve and troubleshoot problems • Communicate and report • Use penetration testing tools effectively • Adapt and customise penetration testing tools and techniques	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Advanced knowledge of cybersecurity attack vectors • Advanced knowledge of IT/OT appliances, operating systems and computer networks • Advanced knowledge of penetration testing tools, techniques and methodologies • Knowledge of scripting and programming languages • Knowledge of security vulnerabilities • Knowledge of best practices on cybersecurity	
e-Competences (from e-CF)	B.2. Component Integration B.3. Testing	Level 4 Level 4

[Source: European cybersecurity skills framework v. 0.5 draft, enisa.europa.eu]

Enisa

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Penetration tester

For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer	B.4. Solution Deployment B.5. Documentation Production E.3. Risk Management	Level 2 Level 3 Level 4

[Source: European cybersecurity skills framework v. 0.5 draft, enisa.europa.eu]

Enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

What was considered during the development of the framework.

During the development of the Framework, there were few principles to be applied:

- The Framework should fit to *European landscape of standardization and legislation*.
- The European Norm (EN) 16234-1 European e-Competence Framework (e-CF) was selected as a reference point. Upcoming Cybersecurity Skills Framework will follow the construction approach of the above-mentioned norm.

[Source: R.2.2.2. Cybersecurity Skills Needs Analysis, REWIRE - Cybersecurity Skills Alliance]

Enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

- The Framework should be simple and made for use of SME‘s (small / medium enterprises) or other non-professionals in the field. This will be reflected in the limited number of profiles.
- The Framework should include only cybersecurity specific **competencies** and **skills**.
General capabilities will not be included in the Framework.

[Source: R.2.2.2. Cybersecurity Skills Needs Analysis, REWIRE - Cybersecurity Skills Alliance]

Enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

What is ECSM?

The European Cybersecurity Month (ECSM) is the European Union's annual campaign dedicated to promoting cybersecurity among EU *citizens* and *organisations*, and to providing *up-to-date online security information* through **awareness** raising and sharing of good practices. Each year, for the entire month of October, hundreds of activities take place across Europe, including conferences, workshops, trainings, webinars, presentations and more, to promote digital **security** and *cyber hygiene*.

[Source: enisa.europa.eu]

Enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

The ECSM campaign is coordinated by the European Union Agency for Cybersecurity (*ENISA*) and the *European Commission*, and supported by EU *Member States* and hundreds of *partners* (governments, universities, think tanks, NGOs, professional associations, private sector business) from *Europe, and beyond*.

[Source: enisa.europa.eu]

Enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

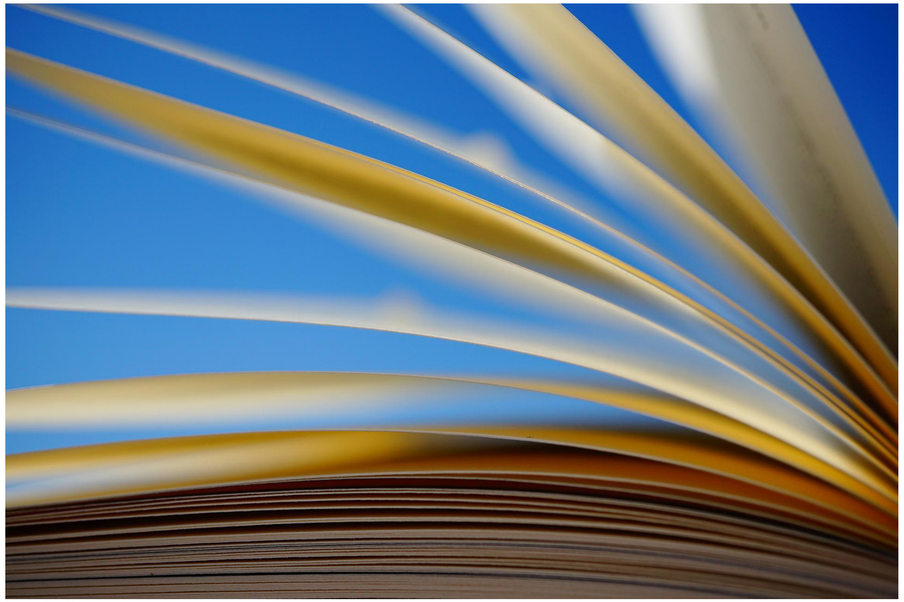
The EU Agency for Cybersecurity coordinates the organisation of the ECSM campaign by acting as a "*hub*" for all participating Member States and EU Institutions, and by providing expert *suggestions*, generating **synergies** and promoting common messaging among EU citizens, businesses and public administration. The Agency also publishes new materials and provides expert advice on different cybersecurity topics for Member States' audiences.

[Source: enisa.europa.eu]

Conclusions

FRAMEWORKS ABOUT COMPETENCIES

An analysis of cybersecurity skills needs requires a widely adopted taxonomy of cybersecurity competencies, also called ‘skills **framework**’. A *competency framework* is based on a comprehensive classification of actual roles, functions and tasks, i.e. the scope of work performed in *day-to-day activities*. Role definitions provide the full scope of "*what specialists in the organization, unit or role are doing*".



Conclusions

FRAMEWORKS ABOUT COMPETENCIES

Frameworks are a form of expression, for companies, academia and institutions, of the demand regarding professional figures in the cyber field, addressed to **students** and **workers**.

Therefore they should make an active contribution in guiding the development of skills.

Conclusions

FRAMEWORKS ABOUT COMPETENCIES

Therefore they should make an active contribution in guiding the development of skills. *How can they do it*?

We have seen that competence can be an **intermediate** *unit* between the *job position* (or title) with its tasks on the one hand and the *KSAs* on the other. Therefore it is appropriate that the skills described are able to reflect and impose themselves *dynamically* on the changing KSAs.

Conclusions

FRAMEWORKS ABOUT COMPETENCIES

In the job market, those who want to be competitive in terms of information security must first of all work very well internally in *defining the objectives pursued in the field of information security and cybersecurity* (see for example ISO/IEC 27001, chap. 5), therefore carry out an **assessment** of internal resources and competences, **understand** what is *missing* to achieve those objectives and therefore open job positions **consistent** *with these purposes*.

Conclusions

FRAMEWORKS ABOUT COMPETENCIES

Sometimes the **meeting** between employer (companies and other organizations) and employees (young students, workers looking for a job) is the most *delicate* moment. Misunderstanding is around the corner, with great **loss** for both the parties. The expectations of the aspiring worker and those of the employer may not coincide.

Conclusions

FRAMEWORKS ABOUT COMPETENCIES

Frameworks, where known by *both parties*, undoubtedly help in this sense and the requirements can be **composed**, **modulated**, based on the context (e.g. we see how the U.S. DoD requires very specific skills, also proven by precise certifications, for access to certain job positions).

University and other institutions that provide for cyber education can play an important role.

Some online resources

Career Pathway roadmap, user guide and resources:

https://niccs.cisa.gov/workforce-development/career-pathway-roadmap

DoD 8570.01-M

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf

European Cybersecurity Skills Framework (April 2022 draft)

https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/ecsf-profiles-v-0-5-draft-release.pdf

Enisa webinar *"Using the European Cybersecurity Skills Framework to sustain cybersecurity workforce"*

https://www.youtube.com/watch?v=yTuWWg_JG64

Enisa cybersecurity Education

https://www.enisa.europa.eu/topics/cybersecurity-education/

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**
Simone **Soderi**
antonio.belli@unipd.it
simone.soderi@unipd.it

Thanks for your attention!

M8 Frameworks that describe the competencies