Mapping NICE work roles 1.0.0 to indicative SFIA 8 skills

Oversight and Governance

NICE Work Role	NICE Work Role Definition	Indicative SFIA Skills
Systems Authorization	Responsible for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the nation.	Information management IRMG Risk management BURM Information security SCTY
Security Control Assessment	Responsible for conducting independent comprehensive assessments of management, operational, and technical security controls and control enhancements employed within or inherited by a system to determine their overall effectiveness.	Information security SCTY Audit AUDT Information assurance INAS Risk management BURM
Cybersecurity Legal Advice	Responsible for providing cybersecurity legal advice and recommendations, including monitoring related legislation and regulations.	Specialist advice TECH
Privacy Compliance	Responsible for developing and overseeing an organization's privacy compliance program and staff, including establishing and managing privacy-related governance, policy, and incident response needs.	Personal data protection PEDP
Cybersecurity Curriculum Development	Responsible for developing, planning, coordinating, and evaluating cybersecurity awareness, training, or education content, methods, and techniques based on instructional needs and requirements.	Learning design and development TMCR Subject formation SUBF Content authoring INCA
Cybersecurity Instruction	Responsible for developing and conducting cybersecurity awareness, training, or education.	Learning delivery ETDL Teaching TEAC Learning design and development TMCR Content authoring INCA
Systems Security Management	Responsible for managing the cybersecurity of a program, organization, system, or enclave.	Information security SCTY Information assurance INAS
Communications Security (COMSEC) Management	Responsible for managing the Communications Security (COMSEC) resources of an organization.	Information assurance INAS Vulnerability assessment VUAS Security operations SCAD
Cybersecurity Workforce Management	Responsible for developing cybersecurity workforce plans, assessments, strategies, and guidance, including cybersecurity-related staff training, education, and hiring processes. Makes adjustments in response to or in anticipation of changes to cybersecurity-related policy, technology, and staffing needs and requirements. Authors mandated workforce planning strategies to maintain compliance with legislation, regulation, and policy.	Workforce planning WFPL Professional development PDSV Learning and development management ETMG Organisation design and implementation ORDI
Cybersecurity Policy and Planning	Responsible for developing and maintaining cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.	Information security SCTY Information assurance INAS Organisational capability development OCDV Workforce planning WFPL

Mapping NICE work roles 1.0.0 to indicative SFIA 8 skills

Design and Development

NICE Work Role	NICE Work Role Definition	Indicative SFIA 8 skills
Secure Software Development	Responsible for developing, creating, modifying, and maintaining computer applications, software, or specialized utility programs.	Programming/software development PROG Testing TEST Software configuration PORT Real-time/embedded systems development RESD Systems integration and build SINT
Secure Software Assessor	Responsible for analyzing the security of new or existing computer applications, software, or specialized utility programs and delivering actionable results.	Vulnerability assessment VUAS Penetration testing PENT
Enterprise Architecture	Responsible for developing and maintaining business, systems, and information processes to support enterprise mission needs. Develops technology rules and requirements that describe baseline and target architectures.	Enterprise and business architecture STPL Requirements definition and management REQM
Cybersecurity Architecture	Responsible for ensuring that security requirements are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems that protect and support organizational mission and business processes.	Information security SCTY Enterprise and business architecture STPL Solution architecture ARCH Requirements definition and management REQM
Technology Research and Development	Responsible for conducting software and systems engineering and software systems research to develop new capabilities with fully integrated cybersecurity. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.	Vulnerability research VURE Research RSCH Emerging technology monitoring EMRG Specialist advice TECH
Systems Requirements Planning	Responsible for consulting with internal and external customers to evaluate and translate functional requirements and integrating security policies into technical solutions.	Requirements definition and management REQM User experience analysis UNAN Solution architecture ARCH
Systems Testing and Evaluation	Responsible for planning, preparing, and executing system tests; evaluating test results against specifications and requirements; and reporting test results and findings.	Testing TEST Quality assurance QUAS Penetration testing PENT User experience evaluation USEV
Secure Systems Development	Responsible for the secure design, development, and testing of systems and the evaluation of system security throughout the systems development life cycle.	Information security SCTY Vulnerability assessment VUAS Continuity management COPL Solution architecture ARCH Systems design DESN Testing TEST Penetration testing PENT

Mapping NICE work roles 1.0.0 to indicative SFIA 8 skills

Implementation and Operation

NICE Work Role	NICE Work Role Definition	Indicative SFIA Skills
Database Administration	Responsible for administering databases and data management systems that allow for the secure storage, query, protection, and utilization of data.	Database administration DBAD Storage management STMG
Data Analysis	Responsible for analyzing data from multiple disparate sources to provide cybersecurity and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.	Data engineering DENG Data modelling and design DTAN Requirements definition and management REQM Data science DATS Business intelligence BINT
Knowledge Management	Responsible for managing and administering processes and tools to identify, document, and access an organization’s intellectual capital.	Knowledge management KNOW Content publishing ICPM
Technical Support	Responsible for providing technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational policies and processes.	Problem management PBMG Security operations SCAD Vulnerability assessment VUAS System software SYSP Network support NTAS System software SYSP Systems installation and removal HSIN IT infrastructure ITOP
Network Operations	Responsible for planning, implementing, and operating network services and systems, including hardware and virtual environments.	System software SYSP Network support NTAS Systems installation and removal HSIN Testing TEST
Systems Administration	Responsible for setting up and maintaining a system or specific components of a system in adherence with organizational security policies and procedures. Includes hardware and software installation, configuration, and updates; user account management; backup and recovery management; and security control implementation.	Security operations SCAD IT infrastructure ITOP Systems installation and removal HSIN System software SYSP Testing TEST Problem management PBMG
Systems Security Analysis	Responsible for developing and analyzing the integration, testing, operations, and maintenance of systems security. Prepares, performs, and manages the security aspects of implementing and operating a system.	Information security SCTY Information assurance INAS Vulnerability assessment VUAS Testing TEST Penetration testing PENT

Mapping NICE work roles 1.0.0 to indicative SFIA 8 skills

Implementation and Operation

NICE Work Role	NICE Work Role Definition	Indicative SFIA Skills
Executive Cybersecurity Leadership	Responsible for establishing vision and direction for an organization's cybersecurity operations and resources and their impact on digital and physical spaces. Possesses authority to make and execute decisions that impact an organization broadly, including policy approval and stakeholder engagement.	Information security SCTY Risk management BURM Information assurance INAS
Program Management	Responsible for leading, coordinating, and the overall success of a defined program. Includes communicating about the program and ensuring alignment with agency or organizational priorities.	Programme management PGMG Quality management QUMG Stakeholder relationship management RLMT Benefits management BENM Organisational change management CIPM Supplier management SUPP
Secure Project Management	Responsible for overseeing and directly managing technology projects. Ensures cybersecurity is built into projects to protect the organization's critical infrastructure and assets, reduce risk, and meet organizational goals. Tracks and communicates project status and demonstrates project value to the organization.	Project management PRMG Service level management SLMO Requirements definition and management REQM Quality management QUMG
Product Support Management	Responsible for planning, estimating costs, budgeting, developing, implementing, and managing product support strategies in order to field and maintain the readiness and operational capability of systems and components.	Service level management SLMO Business situation analysis BUSA Feasibility assessment FEAS Requirements definition and management REQM
Technology Portfolio Management	Responsible for managing a portfolio of technology investments that align with the overall needs of mission and enterprise priorities.	Portfolio management POMG Investment appraisal INVA Stakeholder relationship management RLMT
Technology Program Auditing	Responsible for conducting evaluations of technology programs or their individual components to determine compliance with published standards.	Audit AUDT Information assurance INAS Risk management BURM Quality assurance QUAS

Mapping NICE work roles 1.0.0 to indicative SFIA 8 skills

Protection and Defense

NICE Work Role	NICE Work Role Definition	Indicative SFIA Skills
Threat Analysis	Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat assessments. Develops cybersecurity indicators to maintain awareness of the status of the highly dynamic operating environment.	Threat intelligence THIN Data visualisation VISL Security operations SCAD
Insider Threat Analysis	Responsible for identifying and assessing the capabilities and activities of cybersecurity insider threats; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations.	Threat intelligence THIN Data visualisation VISL Security operations SCAD
Defensive Cybersecurity	Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks.	Threat intelligence THIN Penetration testing PENT
Digital Forensics	Responsible for analyzing digital evidence from computer security incidents to derive useful information in support of system and network vulnerability mitigation.	Digital forensics DGFS Penetration testing PENT Vulnerability assessment VUAS
Infrastructure Support	Responsible for testing, implementing, deploying, maintaining, and administering infrastructure hardware and software for cybersecurity.	Security operations SCAD IT infrastructure ITOP Systems installation and removal HSIN Network support NTAS
Incident Response	Responsible for investigating, analyzing, and responding to network cybersecurity incidents.	Incident management USUP Security operations SCAD Continuity management COPL
Vulnerability Analysis	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.	Vulnerability assessment VUAS Penetration testing PENT Measurement MEAS

Mapping NICE work roles 1.0.0 to indicative SFIA 8 skills

Investigation

NICE Work Role	NICE Work Role Definition	Indicative SFIA Skills
Cybercrime Investigation	Responsible for investigating cyberspace intrusion incidents and crimes. Applies tactics, techniques, and procedures for a full range of investigative tools and processes and appropriately balances the benefits of prosecution versus intelligence gathering.	Digital forensics DGFS
Digital Evidence Analysis	Responsible for identifying, collecting, examining, and preserving digital evidence using controlled and documented analytical and investigative techniques.	Digital forensics DGFS

Mapping NICE work roles 1.0.0 to indicative SFIA 8 skills

Cyberspace Intelligence

NICE Work Role	NICE Work Role Definition	Indicative SFIA Skills
All-Source Analysis	Responsible for analyzing data and information from one or multiple sources to conduct preparation of the operational environment, respond to requests for information, and submit intelligence collection and production requirements in support of intelligence planning and operations.	Threat intelligence THIN Security operations SCAD Vulnerability research VURE
Multi-disciplined Language Analysis	Responsible for applying language and cultural expertise with target, threat, and technical knowledge to process, analyze, and disseminate intelligence information derived from lanugage, voice, and/or graphic materials. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter experise in foreign language-intensive or interdisciplinary projects.	Specialist advice TECH Knowledge management KNOW Vulnerability assessment VUAS Threat intelligence THIN

Mapping NICE work roles 1.0.0 to indicative SFIA 8 skills

Cyberspace Effects

NICE Work Role	NICE Work Role Definition	Indicative SFIA Skills
Exploitation Analysis	Responsible for identifying access and intelligence collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.	Threat intelligence THIN Vulnerability research VURE Penetration testing PENT
Mission Assessment	Responsible for developing assessment plans and performance measures; conducting strategic and operational effectiveness assessments for cyber events; determining whether systems perform as expected; and providing input to the determination of operational effectiveness.	Measurement MEAS Information security SCTY Information assurance INAS Threat intelligence THIN
Target Analysis	Responsible for conducting target development at the system, component, and entity levels. Builds and maintains electronic target folders to include inputs from environment preparation and/or internal or external intelligence sources. Coordinates with partner target working groups and intelligence community members, and presents candidate targets for vetting and validation. Assesses and reports on damage resulting from the application of military force and coordinates federal support as required.	Vulnerability research VURE Threat intelligence THIN Knowledge management KNOW
Target Network Analysis	Responsible for conducting advanced analysis of collection and open-source data to ensure target continuity; profiling targets and their activities; and developing techniques to gain target information. Determines how targets communicate, move, operate, and live based on knowledge of target technologies, digital networks, and applications.	Knowledge management KNOW Data science DATS Penetration testing PENT
All Source-Collection Management	Responsible for identifying intelligence collection authorities and environment; incorporating priority information requirements into intelligence collection management; and developing concepts to meet leadership's intent. Determines capabilities of available intelligence collection assets; constructs and disseminates intelligence collection plans; and monitors execution of intelligence collection tasks to ensure effective execution of collection plans.	Knowledge management KNOW Organisational capability development OCDV Business process improvement BPRE
All Source-Collection Requirements Management	Responsible for evaluating intelligence collection operations and developing effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of intelligence collection requirements. Evaluates performance of intelligence collection assets and operations.	Demand management DEMM Requirements definition and management REQM
Cyber Intelligence Planning	Responsible for developing intelligence plans to satisfy cyber operation requirements. Identifies, validates, and levies requirements for intelligence collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.	Threat intelligence THIN Demand management DEMM Strategic planning ITSP
Cyber Operations Planning	Responsible for developing cybersecurity operations plans; participating in targeting selection, validation, and synchronization; and enabling integration during the execution of cyber actions.	Security operations SCAD Threat intelligence THIN Supplier management SUPP
Partner Integration Planning	Responsible for advancing cooperation across organizaitonal or national borders betwen cyber operations partners. Provides guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.	Stakeholder relationship management RLMT Information security SCTY Knowledge management KNOW
Cyberspace Operations	Responsible for gathering evidence on criminal or foreign intelligence entities to mitigate and protect against possible or real-time threats. Conducts collection, processing, and geolocation of systems to exploit, locate, and track targets. Performs network navigation and tactical forensic analysis and executes on-net operations when directed.	Threat intelligence THIN Digital forensics DGFS