**Matthew Ford Kern versus NICCS Security Architect Standard Knowledge, Skills, and Abilities**

This document compares the Federal Standard security architecture role versus Matthew Kern.

|  |  |
| --- | --- |
| **Abilities** | **# Years** |
| **A0008**: Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]). | **30 years** |
| **A0014**: Ability to communicate effectively when writing. | **30+ years** |
| **A0015**: Ability to conduct vulnerability scans and recognize vulnerabilities in security systems. | **10 years** |
| **A0027**: Ability to apply an organization's goals and objectives to develop and maintain architecture. | **30 years** |
| **A0038**: Ability to optimize systems to meet enterprise performance requirements. | **30 years** |
| **A0048**: Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). | **15 Years** |
| **A0049**: Ability to apply secure system design tools, methods and techniques. | **15 Years** |
| **A0050**: Ability to apply system design tools, methods, and techniques, including automated systems analysis and design tools. | **20 Years** |
| **A0061**: Ability to design architectures and frameworks. | **30 Years** |
| **A0123**: Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). | **30 Years** |
| **A0148**: Ability to serve as the primary liaison between the enterprise architect and the systems security engineer and coordinates with system owners, common control providers, and system security officers on the allocation of security controls as system-specific, hybrid, or common controls. | **20 Years** |
| **A0149**: Ability, in close coordination with system security officers, advise authorizing officials, chief information officers, senior information security officers, and the senior accountable official for risk management/risk executive (function), on a range of security-related issues (e.g. establishing system boundaries; assessing the severity of weaknesses and deficiencies in the system; plans of action and milestones; risk mitigation approaches; security alerts; and potential adverse effects of identified vulnerabilities). | **10 Years** |
| **A0170**: Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations. | **30 Years** |
| **A0172**: Ability to set up a physical or logical sub-networks that separates an internal local area network (LAN) from other untrusted networks. | **10 Years** |
|  |  |
| **Knowledge** | **Education or Training** |
| **K0001**: Knowledge of computer networking concepts and protocols, and network security methodologies. | **CISSP** |
| **K0002**: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). | **CISSP** |
| **K0003**: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. | **CISSP** |
| **K0004**: Knowledge of cybersecurity and privacy principles. | **CISSP** |
| **K0005**: Knowledge of cyber threats and vulnerabilities. | **CISSP** |
| **K0006**: Knowledge of specific operational impacts of cybersecurity lapses. | **CISSP** |
| **K0007**: Knowledge of authentication, authorization, and access control methods. | **CISSP** |
| **K0008**: Knowledge of applicable business processes and operations of customer organizations. | **CEA** |
| **K0009**: Knowledge of application vulnerabilities. | **CISSP** |
| **K0010**: Knowledge of communication methods, principles, and concepts that support the network infrastructure. | **BSEE** |
| **K0011**: Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware. | **BSEE** |
| **K0012**: Knowledge of capabilities and requirements analysis. | **Systems Engineering Courses** |
| **K0013**: Knowledge of cyber defense and vulnerability assessment tools and their capabilities. | **Trade Studies** |
| **K0015**: Knowledge of computer algorithms. | **BSEE, Self Study** |
| **K0018**: Knowledge of encryption algorithms | **CISSP** |
| **K0019**: Knowledge of cryptography and cryptographic key management concepts | **CISSP** |
| **K0024**: Knowledge of database systems. | **Integration Experience** |
| **K0026**: Knowledge of business continuity and disaster recovery continuity of operations plans. | **CISSP** |
| **K0027**: Knowledge of organization's enterprise information security architecture. | **CISSP** |
| **K0030**: Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware). | **BSEE** |
| **K0035**: Knowledge of installation, integration, and optimization of system components. | **Integration Experience** |
| **K0036**: Knowledge of human-computer interaction principles. | **Integration Experience** |
| **K0037**: Knowledge of Security Assessment and Authorization process. | **CISSP** |
| **K0043**: Knowledge of industry-standard and organizationally accepted analysis principles and methods. | **CEA** |
| **K0044**: Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). | **CISSP** |
| **K0052**: Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis). | **BSEE** |
| **K0055**: Knowledge of microprocessors. | **BSEE** |
| **K0056**: Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). | **CISSP** |
| **K0057**: Knowledge of network hardware devices and functions. | **Integration Experience** |
| **K0059**: Knowledge of new and emerging information technology (IT) and cybersecurity technologies. | **Trade Studies** |
| **K0060**: Knowledge of operating systems. | **BSEE** |
| **K0061**: Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]). | **BSEE, MCP, CCNA** |
| **K0063**: Knowledge of parallel and distributed computing concepts. | **BSEE** |
| **K0071**: Knowledge of remote access technology concepts. | **Integration Experience** |
| **K0074**: Knowledge of key concepts in security management (e.g., Release Management, Patch Management). | **CISSP** |
| **K0082**: Knowledge of software engineering. | **Integration Experience** |
| **K0091**: Knowledge of systems testing and evaluation methods. | **Systems Engineering Courses** |
| **K0092**: Knowledge of technology integration processes. | **Integration Experience** |
| **K0093**: Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing). | **BSEE, CCAF Cert** |
| **K0102**: Knowledge of the systems engineering process. | **Systems Engineering Courses** |
| **K0170**: Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations. | **Integration Experience** |
| **K0180**: Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. | **Integration Experience** |
| **K0198**: Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions). | **CEA** |
| **K0200**: Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]). | **ITIL V3** |
| **K0202**: Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing). | **Integration Experience** |
| **K0211**: Knowledge of confidentiality, integrity, and availability requirements. | **CISSP** |
| **K0212**: Knowledge of cybersecurity-enabled software products. | **Trade Studies** |
| **K0214**: Knowledge of the Risk Management Framework Assessment Methodology. | **CISSP, ISSAP** |
| **K0227**: Knowledge of various types of computer architectures. | **BSEE** |
| **K0240**: Knowledge of multi-level security systems and cross domain solutions. | **Integration Experience** |
| **K0260**: Knowledge of Personally Identifiable Information (PII) data security standards. | **CISSP, yearly courses** |
| **K0261**: Knowledge of Payment Card Industry (PCI) data security standards. | **CISSP** |
| **K0262**: Knowledge of Personal Health Information (PHI) data security standards. | **CISSP** |
| **K0264**: Knowledge of program protection planning (e.g. information technology (IT) supply chain security/risk management policies, anti-tampering techniques, and requirements). | **CEA, PMP** |
| **K0275**: Knowledge of configuration management techniques. | **Integration Experience, Technician Experience** |
| **K0277**: Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) security features in databases (e.g. built-in cryptographic key management features). | **CISSP, ISSAP** |
| **K0286**: Knowledge of N-tiered typologies (e.g. including server and client operating systems). | **Integration Experience** |
| **K0287**: Knowledge of an organization's information classification program and procedures for information compromise. | **Classification Courses** |
| **K0291**: Knowledge of the enterprise information technology (IT) architectural concepts and patterns (e.g., baseline, validated design, and target architectures.) | **CEA, Systems Engineering Courses** |
| **K0293**: Knowledge of integrating the organization’s goals and objectives into the architecture. | **CEA** |
| **K0320**: Knowledge of organization's evaluation and validation criteria. | **CEA, Systems Engineering Courses** |
| **K0322**: Knowledge of embedded systems. | **BSEE, Integration Experience, Note Patents** |
| **K0323**: Knowledge of system fault tolerance methodologies. | **BSEE, Technician Experience** |
| **K0325**: Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression). | **BSEE** |
| **K0326**: Knowledge of demilitarized zones. | **CISSP, ISSAP** |
| **K0332**: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. | **CISSP, MCP, CCNA** |
| **K0333**: Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs. | **BSEE, Integration Experience, ISSAP** |
| **K0336**: Knowledge of access authentication methods. | **CISSP, ISSAP** |
| **K0565**: Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications. | **BSEE, ISSAP, MCP, CCNA** |
|  |  |
| **Skills** | **Examples** |
| **S0005**: Skill in applying and incorporating information technologies into proposed solutions. | **100+ Proposals, See Also Systems List** |
| **S0022**: Skill in designing countermeasures to identified security risks. | **ISSO 3x** |
| **S0024**: Skill in designing the integration of hardware and software solutions. | **Systems List** |
| **S0027**: Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. | **Systems List** |
| **S0050**: Skill in design modeling and building use cases (e.g., unified modeling language). | **JSP, Several** |
| **S0059**: Skill in using Virtual Private Network (VPN) devices and encryption. | **Currently use** |
| **S0061**: Skill in writing test plans. | **5 TEP, 20 Test Plans** |
| **S0076**: Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware). | **Treasury, Currently Use, etc.** |
| **S0116**: Skill in designing multi-level security/cross domain solutions. | **PRC, JSP** |
| **S0122**: Skill in the use of design methods. | **All Jobs** |
| **S0138**: Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). | **CGS, JSP** |
| **S0139**: Skill in applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). | **Arcturus, CGS** |
| **S0152**: Skill in translating operational requirements into protection needs (i.e., security controls). | **ISSO 3x** |
| **S0168**: Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from other untrusted networks. | **PRC, Treasury** |
| **S0170**: Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate). | **Currently use** |
| **S0367**: Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). | **DNDO, FEMA** |
| **S0374**: Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations. | **CGS, DNDO** |
|  |  |
| **Tasks** | **Examples** |
| **T0050**: Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. | **FEMA, DNDO, OSD** |
| **T0051**: Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | **FEMA, DNDO, PRC, etc.** |
| **T0071**: Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET). | **DNDO, CGS, PRC** |
| **T0082**: Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle. | **USDA, DOS, CGS** |
| **T0084**: Employ secure configuration management processes. | **PRC, CDC, USAF** |
| **T0090**: Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. |  |
| **T0108**: Identify and prioritize critical business functions in collaboration with organizational stakeholders. | **FEMA, DNDO** |
| **T0177**: Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. | **Teracore, DOS** |
| **T0196**: Provide advice on project costs, design concepts, or design changes. | **PRC** |
| **T0203**: Provide input on security requirements to be included in statements of work and other appropriate procurement documents. | **DNDO, FEMA** |
| **T0205**: Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). | **USDA** |
| **T0268**: Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. | **DNDO, PRC** |
| **T0307**: Analyze candidate architectures, allocate security services, and select security mechanisms. | **ISSO, 3x** |
| **T0314**: Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements. | **DNDO, FEMA, PRC** |
| **T0328**: Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents. | **100+ Proposals** |
| **T0338**: Write detailed functional specifications that document the architecture development process. | **eBooks** |
| **T0427**: Analyze user needs and requirements to plan architecture. | **PRC, Teracore, Interior, Education, FEMA, DNDO, CBP** |
| **T0448**: Develop enterprise architecture or system components required to meet user needs. | **All Architecture Jobs** |
| **T0473**: Document and update as necessary all definition and architecture activities. | **All Architecture Lead and Chief Architect Jobs** |
| **T0484**: Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately. | **ISSO 3x** |
| **T0542**: Translate proposed capabilities into technical requirements. | **PRC, DNDO etc.** |
| **T0556**: Assess and design security management functions as related to cyberspace. | **CGS, JSP** |