

<b>POSITION DESCRIPTION</b>		AGENCY/DEPT ID DAS500000
DIVISION OR INSTITUTION OFFICE OF INFORMATION TECHNOLOGY	UNIT OR OFFICE Office of Security & Privacy	COUNTY OF EMPLOYMENT Franklin

POSITION NUMBER 20075319	<input checked="" type="checkbox"/> Reclassification <input type="checkbox"/> New Position <input type="checkbox"/> Update		Position Hyperlinked to <input type="checkbox"/> Agency Organizational Tree	
	USUAL WORKING TITLE OF POSITION IA Compliance Specialist		POSITION NO. AND TITLE OF IMMEDIATE SUPERVISOR SEE TABLE OF ORGANIZATION	
	<input checked="" type="checkbox"/> Permanent <input type="checkbox"/> Temporary <input type="checkbox"/> Intermittent	<input checked="" type="checkbox"/> Classified <input type="checkbox"/> Unclassified <input type="checkbox"/> Essential	Overtime: <input checked="" type="checkbox"/> Eligible <input type="checkbox"/> Exempt  If FLSA Exempt, exemption type:	Bargaining Unit 14 PR 34 Page 1 of 2
	NORMAL WORKING HOURS (Explain unusual or rotating shift): FROM: 8:00 a.m.    TO: 5:00 p.m. <b>Subject to call 24x7</b>			
<b>JOB DESCRIPTION AND WORKER CHARACTERISTICS</b>				
	%	Job Duties in Order of Importance	Knowledge, Skills & Abilities	
	55	Responsible for evaluating and supporting the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's information assurance and security requirements; ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives; developing methods to monitor and measure risk, compliance, and assurance efforts; developing specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level; drafting statements of preliminary or residual security risks for system operation; continuous monitoring of results/findings to confirm that the level of risk is within acceptable limits for the software application, network, or system; monitor and evaluate agency compliance with IT security, resilience, and dependability requirements; perform validation steps, comparing actual results with expected results and analyze the differences to identify impact and risks; tracks security deficiencies through the documentation of findings and monitor the follow through of remediation efforts; reports on metrics to gauge agency compliance with established reporting requirements; publish periodic metrics report; advising agencies to ensure that the compliance process flows smoothly end-to-end.	<b>Knowledge of</b> (1) Risk Management Framework requirements; (2) Computer Network Defense and vulnerability assessment tools, including open source tools, and their capabilities; (3) current industry methods for evaluating, implementing, and disseminating IT security assessment, monitoring, detection and remediation tools and procedures utilizing standards-based concepts and capabilities; (4) IA principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation); (5) IT supply chain security/risk management policies, requirements, and procedures; (6) known vulnerabilities from alerts, advisories, errata, and bulletins; (7) local specialized system requirements (e.g., critical infrastructure systems for safety, performance, and reliability); (8) network security architecture concepts including topology, protocols, components, and principles (e.g., application of Defense-in-Depth); (9) new and emerging IT and information security technologies; (10) Personally Identifying Information (PII) and personal Payment Card Industry (PCI) data security standards; (11) relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure; (12) structured analysis principles and methods; (13) systems diagnostic tools and fault identification techniques. <b>Skill in</b> (14) 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; (15) evaluating the trustworthiness of the supplier and/or product; (16) identifying measures or indicators of system performance and the actions needed to improve or correct performance relative to the goals of the system.	
	List Position Numbers & Job Titles of Positions Directly Supervised:		SIGNATURE OF AGENCY REPRESENTATIVE  <i>David A Brown</i>	
			DATE 8/25/14	

SPD  
8/25/14

<b>POSITION DESCRIPTION</b>		AGENCY/DEPT ID DAS500000
DIVISION OR INSTITUTION OFFICE OF INFORMATION TECHNOLOGY	UNIT OR OFFICE Office of Security & Privacy	COUNTY OF EMPLOYMENT Franklin

POSITION NUMBER 20075319	<input checked="" type="checkbox"/> Reclassification <input type="checkbox"/> New Position <input type="checkbox"/> Update		Position Hyperlinked to <input type="checkbox"/> Agency Organizational Tree	
	USUAL WORKING TITLE OF POSITION IA Compliance Specialist		POSITION NO. AND TITLE OF IMMEDIATE SUPERVISOR SEE TABLE OF ORGANIZATION	
	<input checked="" type="checkbox"/> Permanent <input type="checkbox"/> Temporary <input type="checkbox"/> Intermittent	<input checked="" type="checkbox"/> Classified <input type="checkbox"/> Unclassified <input type="checkbox"/> Essential	Overtime: <input checked="" type="checkbox"/> Eligible <input type="checkbox"/> Exempt If FLSA Exempt, exemption type:	Bargaining Unit 14 PR 34 Page 2 of 2
	NORMAL WORKING HOURS (Explain unusual or rotating shift): FROM: 8:00 a.m.    TO: 5:00 p.m. <b>Subject to call 24x7</b>			

**JOB DESCRIPTION AND WORKER CHARACTERISTICS**

%	Job Duties in Order of Importance	Knowledge, Skills & Abilities
20	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network; verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations; verify that the software application/network/system accreditation and assurance documentation is current.	<b>Ability to interpret and incorporate data from multiple tool sources; (17) define problems, collect data, establish facts &amp; draw valid conclusions; (18) prepare meaningful, concise &amp; accurate reports; (19) interpret variety of technical computer manuals &amp; documentation; (20) write program specifications &amp; system documentation; (21) communicate verbally &amp; in writing on technical &amp; non-technical matters; (22) cooperate with co-workers on group projects; (23) maintain confidentiality of sensitive information; (24) prioritize &amp; organize assignments; (25) develop &amp; conduct training.</b>  <b>Knowledge of 1-13</b> <b>Skill in 14-16</b> <b>Ability to 17-25</b>
20	Plan and conduct security authorization reviews for initial installation of software applications, systems, and networks; provide an accurate technical evaluation of the software application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant IA compliances; recommend new or revised security, resilience, and dependability measures based on the results of reviews; developing security compliance processes and/or assessments for external services (e.g., cloud service providers, data centers.). Work with state and federal auditors to ensure consistent delivery of audit documentation and remediation of findings.	<b>Knowledge of 1-13</b> <b>Skill in 14-16</b> <b>Ability to 17-25</b>
5	Performs other related duties as needed.	<b>Knowledge of 1-13</b> <b>Skill in 14-16</b> <b>Ability to 17-25</b>

List Position Numbers & Job Titles of Positions Directly Supervised:	SIGNATURE OF AGENCY REPRESENTATIVE <i>David A Brown</i>	DATE 8/25/14
--	--	-----------------

520  
8/25/14

JOB CODE TITLE  
Data Security Analyst 1  
 JOB CODE  
12381  
 APD 10-16-14