

POSITION DESCRIPTION		AGENCY/DEPT ID DAS500000		
DIVISION OR INSTITUTION Office of Information Technology		UNIT OR OFFICE Office of Security & Privacy	COUNTY OF EMPLOYMENT Franklin	
<i>This row is for Information Technology classifications ONLY</i>		PRIMARY TECHNOLOGY (IT ONLY)	SECONDARY TECHNOLOGY (IT ONLY)	
POSITION NUMBER 20090951	<input type="checkbox"/> Reclassification <input checked="" type="checkbox"/> New Position <input type="checkbox"/> Update		Position Hyperlinked to <input type="checkbox"/>	
			Agency Organizational Tree	
	USUAL WORKING TITLE OF POSITION Incident Handler/Forensic Analyst		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	Overtime: <input checked="" type="checkbox"/> Eligible <input type="checkbox"/> Exempt If FLSA Exempt, exemption type:	Bargaining Unit: 14 PR 35 Page 2 of 3
	NORMAL WORKING HOURS (Explain unusual or rotating shift): FROM: _____ TO: _____			
JOB DESCRIPTION AND WORKER CHARACTERISTICS				
%	Job Duties in Order of Importance		Knowledge, Skills & Abilities	
			close-in, distribution, etc.); (19) different operational threat environments; (20) general attack stages; (21) intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies; (22) network traffic analysis methods; (23) packet-level analysis; (24) security event correlation tools; (25) system and application security threats and vulnerabilities. Skills in: (26) performing root cause analysis for incidents; using incident handling methodologies; (27) handling malware; (28) performing damage assessments; (29) preserving evidence integrity according to standard operating procedures or national standards; (30) analyzing anomalous code as malicious or benign; (31) analyzing memory dumps to extract information; (32) analyzing volatile data; (33) collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data; (34) identifying and extracting data of forensic interest in diverse media (media forensics); (35) physically disassembling PCs; (36) setting up a forensic workstation; (37) using binary analysis tools (e.g., Hexedit, xxd, hexdump); (38) using forensic tool suites (e.g., EnCase, Sleuthkit, FTK); (39) using virtual machines * Ability to: (40) Ability to decrypt digital data collections; (41) interpret and incorporate data from multiple tools sources; (42) get along with others.	
JOB CODE 12382		JOB TITLE Data Security Analyst 2		
JOB CODE APD-8-13-15-LMS				
List Position Numbers & Job Titles of Positions Directly Supervised:		SIGNATURE OF AGENCY REPRESENTATIVE <i>David A Brown</i>	DATE 7/23/15	

