

POSITION DESCRIPTION		AGENCY/DEPT ID DAS500000
DIVISION OR INSTITUTION Office of Information Technology	UNIT OR OFFICE Office of Security & Privacy	COUNTY OF EMPLOYMENT Franklin

POSITION NUMBER 20091626	<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 Data Security 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 <input type="checkbox"/> Essential	Overtime: <input checked="" type="checkbox"/> Eligible <input type="checkbox"/> Exempt If FLSA Exempt, exemption type:
NORMAL WORKING HOURS (Explain unusual or rotating shift): Second Shift Position (3:00 PM to 11:00 PM; Monday – Friday)			

JOB DESCRIPTION AND WORKER CHARACTERISTICS		
%	Job Duties in Order of Importance	Knowledge, Skills & Abilities
85	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information; characterize and analyze network traffic to identify anomalous activity and potential threats to network resources; conduct research, analysis and correlation across a wide variety of all source data sets (indications and warnings); conduct tests of Information Assurance safeguards in accordance with established test plans and procedures; provide content development for Computer Network Defense tools; coordinate with enterprise-wide Computer Network Defense staff to validate network alerts; determine appropriate course of action in response to identified and analyzed anomalous network activity; determine tactics techniques and procedures (TTPs) for intrusion sets; document and escalate incidents; Employ approved Defense-in-Depth principles and practices (i.e., Defense in Multiple Places, Layered defenses, Security robustness, etc.); Examine network topologies to understand data flows through the network; identify and analyze anomalies in network traffic using metadata; identify applications and operating systems of a network device based on network traffic; identify network mapping and operating system (OS) fingerprinting activities; monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise; perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack; provide summary reports of network events and activity relevant to Computer Network Defense practices; provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities, receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts; recommend computing environment vulnerability corrections; Reconstruct a malicious attack or activity based off network traffic; triage malware; use Computer Network Defense tools for continual monitoring and analysis of system activity to identify malicious activity; validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.	Knowledge of (1) basic system administration, network, and operating system hardening techniques; (2) *general attack stages (3) host/network access controls; (4)* collection management processes, capabilities, and limitations; (5) common adversary tactics, techniques, and procedures in assigned area of responsibility; (6) data backup, types of backups and recovery concepts and tools; (7) Defense-In-Depth principles and network security architecture; (8)* different classes of attacks (9) cryptology; (10) encryption methodologies; (11) different operational threat environments; (12) different types of network communication (13) file extensions; (14) front-end collection systems, including network traffic collection, filtering, and selection; (15) how traffic flows across the network; (16) IA principles and organizational requirements; (17) incident response and handling methodologies; (18)* intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies; (19) network traffic analysis methods; (20) *new and emerging IT and information security technologies; (21)* system and application security threats and vulnerabilities; (22) troubleshooting basic systems and operating system related issues. Skilled in (23)* detecting host and network-based intrusions via intrusion detection technologies; (24) collecting data from a variety of Computer Network Defense resources; (25) performing packet-level analysis (26) recognizing and categorizing types of vulnerabilities and associated attacks; (27) network analysis tools to identify vulnerabilities. *Developed after employment.

List Position Numbers & Job Titles of Positions Directly Supervised:	SIGNATURE OF AGENCY REPRESENTATIVE 	DATE 10/23/15
--	--	------------------

POSITION NUMBER
20091626

JOB CODE TITLE
Data Security Analyst 1

JOB CODE
12381
Apr 12-1-15 VMB

POSITION DESCRIPTION		AGENCY/DEPT ID DAS500000
DIVISION OR INSTITUTION Office of Information Technology	UNIT OR OFFICE Office of Security & Privacy	COUNTY OF EMPLOYMENT Franklin

POSITION NUMBER 20091626	<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 Data Security 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 <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): Second Shift Position (3:00 PM to 11:00 PM; Monday – Friday)			

JOB DESCRIPTION AND WORKER CHARACTERISTICS

%	Job Duties in Order of Importance	Knowledge, Skills & Abilities
15	Perform other duties as assigned (e.g., work with team lead and assist other staff with various projects; etc.).	<p>Ability to: (28) interpret and incorporate data from multiple tool sources; (29) define problems, collect data, establish facts & draw valid conclusions; (30) prepare meaningful, concise & accurate reports; (31) interpret variety of technical computer manuals & documentation; (32) write program specifications & system documentation; (33) communicate verbally & in writing on technical & non-technical matters; (34) cooperate with co-workers on group projects; (35) maintain confidentiality of sensitive information; (36) prioritize & organize assignments; (37) develop & conduct training.</p> <p>Knowledge of: 1-22* Skill in: 23-27* Ability to: 28-37</p>

*Developed after employment.

List Position Numbers & Job Titles of Positions Directly Supervised:	SIGNATURE OF AGENCY REPRESENTATIVE 	DATE 10/23/15
--	--	------------------

JOB CODE TITLE
 Data Security Analyst 1
 12381
 Apr 12-1-15