

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
20006587

Reclassification New Position Update Position Hyperlinked to Agency Organizational Tree

USUAL WORKING TITLE OF POSITION: Computer Network Defense Analyst POSITION NO. AND TITLE OF IMMEDIATE SUPERVISOR: SEE TABLE OF ORGANIZATION

Permanent Classified Overtime: Eligible Exempt Bargaining Unit 22
 Temporary Unclassified
 Intermittent Essential If FLSA Exempt, exemption type: PR 34
Page 2 of 2

NORMAL WORKING HOURS (Explain unusual or rotating shift):
FROM: 8:00 a.m. TO: 5:00 p.m. Subject to call 24x7

JOB DESCRIPTION AND WORKER CHARACTERISTICS

%	Job Duties in Order of Importance	Knowledge, Skills & Abilities
	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.	Analysis (26) recognizing and categorizing types of vulnerabilities and associated attacks; (27) network analysis tools to identify vulnerabilities Ability to: interpret and incorporate data from multiple tool sources; (28) define problems, collect data, establish facts & draw valid conclusions; (29) prepare meaningful, concise & accurate reports; (30) interpret variety of technical computer manuals & documentation; (31) write program specifications & system documentation; (32) communicate verbally & in writing on technical & non-technical matters; (33) cooperate with co-workers on group projects; (34) maintain confidentiality of sensitive information; (35) prioritize & organize assignments; (36) develop & conduct training.
10	Conduct threat and incident briefings for agency management, homeland security personnel, law enforcement, and external partners.	Knowledge of: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22 Skill in: 23, 24, 25, 26, 27 Ability to: 28, 29, 30, 31, 32, 33, 34, 35, 36
10	Performs other related duties as needed: work as a team lead and assist other staff when needed.	Knowledge of: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22 Skill in: 23, 24, 25, 26, 27 Ability to: 28, 29, 30, 31, 32, 33, 34, 35, 36

JOB CODE TITLE
Data Security Analyst 1

APP 10-16-14

JOB CODE
12381

List Position Numbers & Job Titles of Positions Directly Supervised:

SIGNATURE OF AGENCY REPRESENTATIVE

DATE

David A Brown

8/25/14

SRD
8/25/14