

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 20092240	<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 Supervisor		POSITION NO. AND TITLE OF IMMEDIATE SUPERVISOR SEE TABLE OF ORGANIZATION
<input checked="" type="checkbox"/> Permanent <input checked="" type="checkbox"/> Classified <input type="checkbox"/> Temporary <input type="checkbox"/> Unclassified <input type="checkbox"/> Intermittent <input type="checkbox"/> Essential		Overtime: <input type="checkbox"/> Eligible <input checked="" type="checkbox"/> Exempt	Bargaining Unit 22 PR 15 Page 1 of 3
If FLSA Exempt, exemption type:			
NORMAL WORKING HOURS (Explain unusual or rotating shift): SECOND SHIFT (Monday-Friday: 3:00pm - 12:00 a.m.)			

JOB DESCRIPTION AND WORKER CHARACTERISTICS		
%	Job Duties in Order of Importance	Knowledge, Skills & Abilities
50	<p>Directs Data Security Analysts and Data Security Specialists in the analysis of identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information; characterizes and analyzes network traffic to identify anomalous activity and potential threats to network resources; conducts research, analysis and correlation across a wide variety of all source data sets (indications and warnings); coordinates with other security and system/network administrator staff to validate network alerts; determines appropriate course of action in response to identified and analyzed anomalous network activity; determines tactics techniques and procedures (TTPs) for intrusion sets; documents and escalates incidents; employs approved Defense-in-Depth principles and practices (i.e., Defense in Multiple Places, Layered defenses, Security robustness, etc.); examines network topologies to understand data flows through the network; identifies and analyzes anomalies in network traffic; identifies network mapping and operating system (OS) fingerprinting activities; monitors 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 determines which security issues may have an impact on the enterprise; performs Computer Network Defense trend analysis and reporting; performs 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.</p>	<p>Knowledge of: (1) applicable laws (e.g. Electronic Communications Privacy act, search and seizure laws, civil liberties and privacy laws, etc.) statutes, and or administrative/criminal legal guidelines & procedure relevant to work performed; (2) basic system administration, network and operating system hardening techniques; (3) collection management processes, capabilities and limitations; (4) common adversary tactics, techniques and procedures in assigned area of responsibility; (5) common network tools; (6) Computer Network Defense and vulnerability assessment tools including open source tools, and their capabilities; (7) Computer Network Defense policies, procedures and regulations; (8) content development (9) data backup, types of backups; (10) Defense-In-Depth principles and network security architecture; (11) different classes of attacks; (12) different operational threat environments; (13) different types of network communications; (14) encryption methodologies; (15) file extensions; (16) front-end collection systems, including network traffic collection, filtering and selection; (17) general attach stages; (18) host/network access controls; (19) how traffic flows across the network; (20) IA principles and organizational requirements; (21) incident response and handling methodologies; (21) intrusion detection methodologies and techniques for detecting host and network based intrusions via intrusion detection</p>

JOB CODE 12385	List Position Numbers & Job Titles of Positions Directly Supervised: See table of organization.	SIGNATURE OF AGENCY REPRESENTATIVE <i>David Q Brown</i>	DATE ^{SD} <i>2/29/16</i>

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 20092240	<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 Supervisor		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 type="checkbox"/> Eligible <input checked="" type="checkbox"/> Exempt If FLSA Exempt, exemption type:	Bargaining Unit 22 PR 15 Page 3 of 3							
	NORMAL WORKING HOURS (Explain unusual or rotating shift): SECOND SHIFT (Monday-Friday: 3:00pm - 12:00 a.m.)										
JOB DESCRIPTION AND WORKER CHARACTERISTICS											
JOB CODE 12385	JOB CODE TITLE Data Security Supervisor 1	%	<table border="1"> <thead> <tr> <th>Job Duties in Order of Importance</th> <th>Knowledge, Skills & Abilities</th> </tr> </thead> <tbody> <tr> <td>30 Provides daily summary reports of network events and activity relevant to Computer Network Defense practices; provides timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguishes these incidents and events from benign activities; Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts; reconstructs a malicious attack or activity based off network traffic; triages malware; uses Computer Network Defense tools for continual monitoring and analysis of system activity to identify malicious activity; validates intrusion detection system (IDS) alerts against network traffic using packet analysis tools.</td> <td> categorizing types of vulnerabilities and associated attacks; (49) using incident handling methodologies; (50) using network analysis tools to identify vulnerabilities; (51) using protocol analyzers; (52) using subnetting tools; (53) utilizing virtual networks for testing. Ability to: (54) interpret and incorporate data from multiple tools sources. Knowledge of: 1-37 Skill in: 38-53 Ability to: 54 </td> </tr> <tr> <td>10 Develops security monitoring and incident response procedures. Provides training to personnel on security policies and procedures. Develops training exercises for security personnel on incident analysis, handling, and response.</td> <td> Knowledge of: 1-37 Skill in: 38-53 Ability to: 54 </td> </tr> <tr> <td>10 Schedules employees and maintains sufficient staffing levels for security monitoring functions. Performs other supervisory duties such as evaluating employee performance, interview and recommend candidates for employment, developing work priorities and reporting on unit activities. Performs other duties as assigned</td> <td> Knowledge of: 1-37 Skill in: 38-53 Ability to: 54 </td> </tr> </tbody> </table>	Job Duties in Order of Importance	Knowledge, Skills & Abilities	30 Provides daily summary reports of network events and activity relevant to Computer Network Defense practices; provides timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguishes these incidents and events from benign activities; Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts; reconstructs a malicious attack or activity based off network traffic; triages malware; uses Computer Network Defense tools for continual monitoring and analysis of system activity to identify malicious activity; validates intrusion detection system (IDS) alerts against network traffic using packet analysis tools.	categorizing types of vulnerabilities and associated attacks; (49) using incident handling methodologies; (50) using network analysis tools to identify vulnerabilities; (51) using protocol analyzers; (52) using subnetting tools; (53) utilizing virtual networks for testing. Ability to: (54) interpret and incorporate data from multiple tools sources. Knowledge of: 1-37 Skill in: 38-53 Ability to: 54	10 Develops security monitoring and incident response procedures. Provides training to personnel on security policies and procedures. Develops training exercises for security personnel on incident analysis, handling, and response.	Knowledge of: 1-37 Skill in: 38-53 Ability to: 54	10 Schedules employees and maintains sufficient staffing levels for security monitoring functions. Performs other supervisory duties such as evaluating employee performance, interview and recommend candidates for employment, developing work priorities and reporting on unit activities. Performs other duties as assigned	Knowledge of: 1-37 Skill in: 38-53 Ability to: 54
Job Duties in Order of Importance	Knowledge, Skills & Abilities										
30 Provides daily summary reports of network events and activity relevant to Computer Network Defense practices; provides timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguishes these incidents and events from benign activities; Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts; reconstructs a malicious attack or activity based off network traffic; triages malware; uses Computer Network Defense tools for continual monitoring and analysis of system activity to identify malicious activity; validates intrusion detection system (IDS) alerts against network traffic using packet analysis tools.	categorizing types of vulnerabilities and associated attacks; (49) using incident handling methodologies; (50) using network analysis tools to identify vulnerabilities; (51) using protocol analyzers; (52) using subnetting tools; (53) utilizing virtual networks for testing. Ability to: (54) interpret and incorporate data from multiple tools sources. Knowledge of: 1-37 Skill in: 38-53 Ability to: 54										
10 Develops security monitoring and incident response procedures. Provides training to personnel on security policies and procedures. Develops training exercises for security personnel on incident analysis, handling, and response.	Knowledge of: 1-37 Skill in: 38-53 Ability to: 54										
10 Schedules employees and maintains sufficient staffing levels for security monitoring functions. Performs other supervisory duties such as evaluating employee performance, interview and recommend candidates for employment, developing work priorities and reporting on unit activities. Performs other duties as assigned	Knowledge of: 1-37 Skill in: 38-53 Ability to: 54										
List Position Numbers & Job Titles of Positions Directly Supervised: See table of organization.		SIGNATURE OF AGENCY REPRESENTATIVE <i>David A Brown</i>	DATE 2/29/16								