

POSITION DESCRIPTION

AGENCY/DEPT ID
DAS501710

DIVISION OR INSTITUTION
Office of Information Technology

UNIT OR OFFICE
Office of Security & Privacy

COUNTY OF EMPLOYMENT
Franklin

POSITION NUMBER
20006327

Reclassification

New Position

Update

Position Hyperlinked to

Agency Organizational Tree

USUAL WORKING TITLE OF POSITION
Data Security Supervisor

POSITION NO. AND TITLE OF IMMEDIATE SUPERVISOR
SEE TABLE OF ORGANIZATION

Permanent
 Temporary
 Intermittent

Classified
 Unclassified
 Essential

Overtime: Eligible Exempt
If FLSA Exempt, exemption type:

Bargaining Unit 22
PR 15
Page 1 of 3

NORMAL WORKING HOURS (Explain unusual or rotating shift):
FROM: 8:00 a.m. TO: 5:00 p.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; provides daily summary reports of network events and activity relevant to Computer Network Defense practices; provides timely detection,</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 mythologies; (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 TITLE
Data Security Supervisor 1

JOB CODE
12385
APD 12-12-13 VAS

List Position Numbers & Job Titles of Positions Directly Supervised:

SIGNATURE OF AGENCY REPRESENTATIVE

DATE

David A Brown

12/4/13
SPD 12/4/13

POSITION DESCRIPTION

AGENCY/DEPT ID
DAS501710

DIVISION OR INSTITUTION
Office of Information Technology

UNIT OR OFFICE
Office of Security & Privacy

COUNTY OF EMPLOYMENT
Franklin

POSITION NUMBER
20006327

Reclassification New Position Update Position Hyperlinked to Agency Organizational Tree

USUAL WORKING TITLE OF POSITION: Data Security Supervisor 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 15
Page 2 of 3

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

JOB DESCRIPTION AND WORKER CHARACTERISTICS

%	Job Duties in Order of Importance	Knowledge, Skills & Abilities
	<p>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.</p>	<p>A technologies; (22) Intrusion detection system tools and applications; (23) network protocols such as TCP/IP, Dynamic Host Configuration, Domain name Systems and directory services; (24) network security architecture concepts including topology, protocols, components and principles; (25) network traffic analysis methods; (26) new and emerging IT and information security technologies; (27) penetration testing principles, tools and techniques; (28) policy based and risk adaptive access controls; (29) security management; (30) signature implementation impact; (31) system and application security threats and vulnerabilities; (32) the common attack vectors on the network layer; (33) troubleshooting basic systems and operating system related issues; (34) VPN Security; (35) what constitutes a network attack and the relationship to both threats and vulnerabilities; (36) windows command line; (37) Windows/Unix ports and services. Skill in: (38) collecting data from a variety of Computer Network Defense resources; (39) conducting open source research for troubleshooting novel client-level problems; (40) configuring and utilizing network-based protection components; (41) data reduction; (42) detecting host and network based intrusions via intrusion detection technologies; (43) developing and deploying signatures; (44) identifying common encoding techniques; (45) network mapping an recreating network topologies; (46) performing packet-level analysis; (47) reading and interpreting signatures; (48) recognizing and</p>

JOB CODE TITLE
Data Security Supervisor 1

JOB CODE
12385
APP 12-12-13 VAS

List Position Numbers & Job Titles of Positions Directly Supervised:

SIGNATURE OF AGENCY REPRESENTATIVE

DATE

David A Brown

12/4/13
2/4/13

POSITION DESCRIPTION

AGENCY/DEPT ID
DAS501710

DIVISION OR INSTITUTION
Office of Information Technology

UNIT OR OFFICE
Office of Security & Privacy

COUNTY OF EMPLOYMENT
Franklin

POSITION NUMBER
20006327

Reclassification

New Position

Update

Position Hyperlinked to

Agency Organizational Tree

USUAL WORKING TITLE OF POSITION
Data Security Supervisor

POSITION NO. AND TITLE OF IMMEDIATE SUPERVISOR
SEE TABLE OF ORGANIZATION

Permanent
 Temporary
 Intermittent

Classified
 Unclassified
 Essential

Overtime: Eligible Exempt
If FLSA Exempt, exemption type:

Bargaining Unit 22
PR 15
Page 3 of 3

NORMAL WORKING HOURS (Explain unusual or rotating shift):

FROM: 8:00 a.m. TO: 5:00 p.m.

JOB DESCRIPTION AND WORKER CHARACTERISTICS

%	Job Duties in Order of Importance	Knowledge, Skills & Abilities
		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.
20	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.	
15	Provides threat briefings to senior management, Ohio Homeland Security, and other partners. Coordinates distribution of cyber intelligence information to IT security personnel. Participates in meetings with the Multi-State Information Sharing & Analysis Center, US Department of Homeland Security, and other partners.	
15	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	
*	c	

JOB CODE TITLE
Data Security Supervisor 1

JOB CODE
12385
APD 12-12-13 UAD

List Position Numbers & Job Titles of Positions Directly Supervised:

SIGNATURE OF AGENCY REPRESENTATIVE

DATE
12/4/13

David A. Brown

520, 21 1/13