



<b>POSITION DESCRIPTION</b>		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)	
<b>POSITION NUMBER</b> 20090951	<input type="checkbox"/> Reclassification <input type="checkbox"/> New Position <input checked="" type="checkbox"/> Update		Position Hyperlinked to <input type="checkbox"/> Agency Organizational Tree	
	<b>USUAL WORKING TITLE OF POSITION</b> Incident Handler/Forensic Analyst		<b>POSITION NO. AND TITLE OF IMMEDIATE SUPERVISOR</b> 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: _____			
	<b>JOB DESCRIPTION AND WORKER CHARACTERISTICS</b>			
%	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. <b>Skills in:</b> (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 * <b>Ability to:</b> (40) Ability to decrypt digital data collections; (41) interpret and incorporate data from multiple tools sources; (42) get along with others.	
List Position Numbers & Job Titles of Positions Directly Supervised:		SIGNATURE OF AGENCY REPRESENTATIVE	DATE	
<b>JOB TITLE</b> Data Security Analyst 2				
<b>JOB CODE</b> 12363				

# POSITION DESCRIPTION

AGENCY/DEPT ID  
DAS500000

DIVISION OR INSTITUTION  
Office of Information Technology

UNIT OR OFFICE  
Office of Security & Privacy

COUNTY OF EMPLOYMENT  
Franklin

*This row is for Information Technology classifications ONLY*

PRIMARY TECHNOLOGY (IT ONLY)

SECONDARY TECHNOLOGY (IT ONLY)

Reclassification

New Position

Update

Position Hyperlinked to

Agency Organizational Tree

USUAL WORKING TITLE OF POSITION  
Incident Handler/Forensic Analyst

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

Permanent  
 Temporary  
 Intermittent

Classified  
 Unclassified

Overtime:  Eligible  Exempt

Bargaining Unit: 14

PR 35

Page 3 of 3

If FLSA Exempt, exemption type:

NORMAL WORKING HOURS (Explain unusual or rotating shift):  
FROM: TO:

## JOB DESCRIPTION AND WORKER CHARACTERISTICS

%	Job Duties in Order of Importance	Knowledge, Skills & Abilities
20	Create a forensically sound duplicate of the evidence (forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CD, PDA, mobile phones, GPS, and all tape formats; Perform file system forensic analysis; Perform hash comparison against established database; Perform live forensic analysis (e.g., using Helix in conjunction with LiveView); Recognize and accurately report forensic artifacts indicative of a particular operating system; Review forensic images and other data sources for recovery of potentially relevant information; Utilize deployable forensics tool kit to support operations as necessary; Formulate a strategy to ensure chain of custody is maintained in such a way that the evidence is not altered (ex: phones/PDAs need a power source, hard drives need protection from shock and strong magnetic fields); Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	Knowledge of: 1-25 Skill in 26-39 Ability to 40 - 42
10	Performs other related duties as needed: work as a team lead and assist other staff when needed. Assist lower level data security personnel in incident response and incident analysis processes.	Knowledge of: 1-25 Skill in 26-39 Ability to 40 - 42
*This position requires the employee to be able to obtain a SECRET level U.S. Government security clearance.		

POSITION NUMBER  
20090951

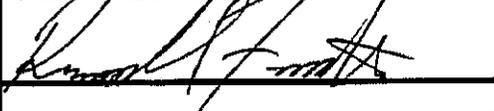
JOB TITLE  
Data Security Analyst 2

JOB CODE  
12383

List Position Numbers & Job Titles of Positions Directly Supervised:

SIGNATURE OF AGENCY REPRESENTATIVE

DATE



3/16/16

