

IT Specialist (Information Security) IT Specialist (Information Security) Fuquay-Varina, NC
Authorized to work in the US for any employer Work Experience IT Specialist (Information Security)
Environmental Protection Agency (EPA) - Durham, NC February 2016 to Present IT Security Analyst
Enterprise Holdings - St. Louis, MO August 2014 to January 2016 IT Specialist (Information
Security) U.S. Department of Agriculture - National Finance Center - New Orleans, LA July 2012 to
July 2014 Education Master's in Information Technology University of North Carolina at Charlotte -
Charlotte, NC January 2010 to December 2011 Graduate Certificate in Information Security and
Privacy University of North Carolina at Charlotte - Charlotte, NC January 2010 to December 2011
Bachelor's in Software and Information Systems University of North Carolina at Charlotte -
Charlotte, NC January 2007 to December 2009 Awards National Science Foundation - Federal
Cyber Security Scholarship (SFS) 2009-12 Certifications/Licenses Certified Information Systems
Security Professional (CISSP) August 2016 to Present GIAC Certified Intrusion Analyst August 2015
to Present Tenable Certified Security Engineer April 2013 to April 2014 CompTIA Security+ March
2012 to March 2015 Additional Information Experienced with discovering and correlating security
incidents using IDS, DLP, and SIEM technologies Used Splunk frequently as a compliance and
incident response investigation tool to correlate various syslogs and network logs Involved with
customization and tuning of a Data Loss Prevention system to more accurately detect threats and
potential loss of agency personal identifiable information Tuned and monitored Web Application
Firewall for various websites that were continuously being upgraded and modified Provided IT
Compliance reports using asset management systems and vulnerability scans (i.e. Tivoli Endpoint
Manager (BigFix), Nessus) Performed forensic analysis using the Forensic Toolkit software and
manual analysis of the Windows Registry in cases where employee workstation misuse was
suspected Used various open source and proprietary tools to conduct static behavioral RAM
analysis for malware and analyzing volatile evidence (i.e. Volatility and Redline) Developed
Security Risk Analyses for customer requested IT products, suggested security products, and
identified security vulnerabilities Discovered software vulnerabilities as a result of incident
response investigations Conducted security awareness training for users, help desk employees,

and administrators Frequently developed and update NIST driven information security standard
operating procedures, policies, and directives Managed POA&Ms for security related projects
being implemented by administrators, Software/Hardware Waiver requests, and Acceptable Risk
documentation Researched methods to detect previously unidentifiable unauthorized network
traffic (i.e. encrypted Tor traffic) Prepared requirement gathering questions to identify security
tools that provided the most value across other internal IT groups Addressed and closed network
security audit findings Provided security feedback as an active member of the Firewall Review
Board for firewall requests

Name: Alyssa Johnson

Email: frankfleming@example.com

Phone: 8032764156